NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NATO'S PREPAREDNESS FOR CYBERWAR

by

Z'hra M. Ghavam

September 2016

Thesis Advisor: David Yost
Co-Advisor: Rodrigo Nieto-Gomez

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE NATO'S PREPAREDNESS FOR CYBERWAR			**5. FUNDING NUMBERS**
6. AUTHOR(S) Z'hra M. Ghavam			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The advent of cyberspace has created a new, unregulated dimension of warfare, which the North Atlantic Treaty Organization (NATO) has striven to manage. This thesis raises the following question: To what extent is NATO cybernetically, politically, militarily, and economically prepared to respond to a major act of cyberwar against one or more of its members? The thesis evaluates NATO's level of preparedness across seven areas: cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization. The thesis concludes that NATO is moderately prepared to respond effectively to a major act of cyberwar launched against one or more of the Allies. NATO's implementation of its cyber policies and cooperative partnerships probably make it cybernetically prepared to address major acts of cyberwar; however, challenges with decision making, public support, crisis management, defense spending, and defense policies could make NATO less than optimally effective in responding with force to acts of cyber aggression that rise to the level of a conventional armed attack. The thesis recommends that NATO enhance its efforts in cyber strategy development, cyber cooperation, decisional delegation, strategic messaging, and defense spending to address challenges resulting from the evolving complexity and heterogeneity of cyber incidents.

14. SUBJECT TERMS North Atlantic Treaty Organization, NATO, Washington Treaty, North Atlantic Treaty, Article 5, collective defense, consensus, cyber, cyber attack, cyberwar, cybersecurity, hybrid, cyber readiness, conventional armed attack, kinetic attack, Wales Summit, Warsaw Summit			**15. NUMBER OF PAGES** 141
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

NATO'S PREPAREDNESS FOR CYBERWAR

Z'hra M. Ghavam
Lieutenant Commander, United States Navy
B.S., United States Naval Academy, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
EUROPE AND EURASIA**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2016**

Approved by: David Yost, Ph.D.
Thesis Advisor

Rodrigo Nieto-Gomez, Ph.D.
Co-Advisor

Mohammed M. Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The advent of cyberspace has created a new, unregulated dimension of warfare, which the North Atlantic Treaty Organization (NATO) has striven to manage. This thesis raises the following question: To what extent is NATO cybernetically, politically, militarily, and economically prepared to respond to a major act of cyberwar against one or more of its members? The thesis evaluates NATO's level of preparedness across seven areas: cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization. The thesis concludes that NATO is moderately prepared to respond effectively to a major act of cyberwar launched against one or more of the Allies. NATO's implementation of its cyber policies and cooperative partnerships probably make it cybernetically prepared to address major acts of cyberwar; however, challenges with decision making, public support, crisis management, defense spending, and defense policies could make NATO less than optimally effective in responding with force to acts of cyber aggression that rise to the level of a conventional armed attack. The thesis recommends that NATO enhance its efforts in cyber strategy development, cyber cooperation, decisional delegation, strategic messaging, and defense spending to address challenges resulting from the evolving complexity and heterogeneity of cyber incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ANA	Afghan National Army
ANSF	Afghan National Security Force
BAP	Baltic Air Policing
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Information
CAR	Central African Republic
CCDCOE	Cooperative Cyber Defense Center of Excellence
CDMA	Cyber Defense Management Authority
CERT	Computer Emergency Response Team
CIS	Communications and Information Systems
CTAC	Cyber Threat Analysis Cell
DDoS	Distributed Denial-of-Service
DIME	Diplomacy, Information, Military, and Economics
DOD	Department of Defense
ENISA	European Union Agency for Network and Information Security
EU	European Union
EW	Electronic Warfare
GBP	British Pound Sterling
HQC3	Headquarters Consultation, Control and Communications
ICT	Information and Communications Technology
IFOR	Implementation Force
IP	Internet Protocol
ISAF	International Security Assistance Force
ISIL	Islamic State of Iraq and the Levant
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITU	International Telecommunication Union
MC	Military Committee
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization

NCIA	NATO Communications and Information Agency
NCIO	NATO Communications and Information Organization
NCIRC	NATO Computer Incident Response Capability
NEO	Non-combatant Evacuation Operation
NGO	Non-Governmental Organization
NRF	NATO Reaction Force
NSS	National Security Strategy
OOA	Out-of-Area Operation
OPM	Office of Personnel Management
OSCE	Organization for Security and Cooperation in Europe
PING	Packet Internet Groper
R&D	Research and Development
RRT	Rapid Reaction Team
SDSR	Strategic Defense and Security Review
SFOR	Stabilization Force
SHAPE	Supreme Headquarters Allied Powers Europe
SPS	Science for Peace and Security
UK	United Kingdom
UN	United Nations
UNPROFOR	United Nations Protection Force
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
USD	U.S. Dollar
VHRJTF	Very High Readiness Joint Task Force

ACKNOWLEDGMENTS

This thesis could not have been completed without the support of others who have guided me throughout the entirety of this process. First and foremost, I would like to thank and venerate God the Father for blessing me with spiritual guidance, good health, and creative inspiration throughout the past 16 months of research and writing. I would also like to thank my family, namely my mother, Dr. Carolyn Ghavam, and my beloved, Luis Armando, for motivating me to reach beyond my perceived limits. Their love, encouragement, and consideration helped foster a home environment that was most conducive to my cognitive processes.

The faculty and staff at the Naval Postgraduate School have also been instrumental to the completion of this project. I would especially like to express my deepest gratitude and thanks to my thesis advisor, Dr. David Yost, for sharing with me his expertise on NATO policy and doctrine. The countless hours he dedicated to mentoring and working with me during detailed and comprehensive reviews contributed considerably to the refined work of scholarship produced. I would like to express my sincerest appreciation to my co-advisor, Dr. Rodrigo Nieto-Gomez, for providing critical feedback and technical assistance on the cyber components of this thesis. I would also like to thank Dr. Wade Huntley for first stimulating my interest in the academic study of NATO's cyberwarfare capabilities and readiness. In addition, I am grateful to Dr. James Wirtz, Dr. Donald Abenheim, and Captain Erik Stohlmann, United States Navy, for affording me the opportunity to visit NATO Headquarters in Brussels, Belgium, which deepened my professional insight on the topic of NATO's cyber preparedness and enriched the scope of this research. Finally, I am indebted to many key individuals within the U.S. Mission to NATO, the Supreme Headquarters Allied Powers Europe (SHAPE), the Military Delegation, the Public Diplomacy Division, and the cyber defense divisions within the NATO Communications and Information Organization (NCIO)**,** for taking time out of their demanding schedules to answer the questions of an inquisitive graduate student. Their efforts are profoundly appreciated.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The advent of cyberspace has created a new, unregulated dimension of warfare, which the North Atlantic Treaty Organization (NATO) has striven to define and manage. Over the years, the Alliance has taken great strides to modernize its framework to meet cybersecurity challenges. At the Wales Summit in September 2014, NATO made an unprecedented declaration: cyber defense would become a component of its core task of collective defense.[1] This announcement came at a time of pronounced cyber aggression toward Alliance members, which has raised questions about NATO's readiness to respond to major threats in cyberspace.

A. RESEARCH QUESTIONS

This thesis raises the following research questions: To what extent is NATO cybernetically, politically, militarily, and economically prepared to respond effectively to a major act of cyber aggression launched against one or more of its members? How have cyber attacks against NATO Allies and partners influenced the Alliance, and how has the Alliance responded? To what extent has NATO adapted organizationally to respond to cyber aggression? In the case of a cyberwar that transcended the cyber dimension and extended into the physical dimension of kinetic operations, would the Alliance be ready to respond decisively with force?

The study focuses on the evolution of the Alliance against a backdrop of cyberwarfare campaigns launched in its own backyard, including in Georgia and Ukraine. Furthermore, it discusses NATO's cyber achievements and the factors that complicate the formulation and implementation of more effective Alliance responses to cybersecurity challenges. It also assesses how prepared NATO is to respond cybernetically, politically, and kinetically against adversaries who initiate aggression via cyberspace. Finally, the thesis examines the conditions under which NATO is more likely to respond with

[1] "Wales Summit Declaration," NATO, September 5, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, par. 72.

collective defense measures to a major act of cyberwar and considers whether these measures would necessarily involve the use of force.

B. SIGNIFICANCE OF THE RESEARCH QUESTIONS

Cyberspace is a physical and virtual domain that is comprised of computer hardware, information infrastructure, and electronic systems, which make digital interactions and communications possible.[2] The cyber dimension has emerged as one of the most indispensable and yet vulnerable domains. Cyber attackers have increased digital attacks against both private industry and state actors to fulfill various political, informational, military, and financial agendas.[3] Cyber attacks against critical infrastructure—that is, systems, networks, organizational structures, and resources vital to a nation's security and well-being—have the power to destabilize organizations, industries, and nations.[4] For most NATO members, the vulnerability of critical infrastructure and information systems within the energy, financial, telecommunications, and health sectors represents the leading concern.[5]

An act of cyber aggression on a nation's financial industry could trigger a regional economic crisis. A cyber attack that releases sensitive information on a presidential candidate could influence the results of a ballot decision, corrupt the institutional integrity of nationally held elections, and even prompt regime change. Moreover, a cyber attack that disabled a country's power grid or contaminated its water supply could create social havoc and paralyze national activity. The Center for Strategic and International Studies has shown the ubiquity of cyber threats by publishing reports on major cyber incidents involving espionage and attacks committed by state and non-state agents. Some of the organizations and industries that have incurred significant cyber

---

[2] Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 2.

[3] Jens Stoltenberg, "NATO and Cyber Attacks: Time to Raise Our Game," *The Parliament*, July 29, 2016, https://www.theparliamentmagazine.eu/blog/nato-and-cyber-attacks-time-raise-our-game, 1.

[4] The White House, *Critical Infrastructure Security and Resilience*, PPD-21, Washington, DC: Office of the Press Secretary, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, 1.

[5] Benjamin S. Buckland, Fred Schreier, and Theodor H. Winkler, "Democratic Governance Challenges of Cybersecurity," DCAF Horizon 2015 Working Paper, no.1, 2015, http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security, 9.

intrusions and attacks include the U.S. Democratic National Committee (2016), the U.S. Joint Chiefs of Staff (2015), the White House (2014, 2015), the U.S. State Department (2006, 2014), Sony Pictures Entertainment (2014), the U.S. Office of Personnel Management (2014), the U.S. Department of Energy (2014), the European Aeronautic Defense and Space Company (2013), 23 U.S. gas pipelines (2011-2012), Google (2010, 2011), NASA (2011), the International Monetary Fund (2011), the European Commission (2011), the European Union (2011), and NASDAQ (2010).[6] While these examples provide a glimpse of the power of cybernetic weapons, they also show that cyberspace represents much more than just another military conduit of modern warfare.

Policy makers and members of the military use the DIME principle to discuss the four ways through which a nation develops and projects its power: diplomacy, information, the military, and economics. Up until now, this principle was sufficient to address the primary instruments of state power; however, it overlooks the cyber domain, which touches all four areas—not just the informational or military spheres. Not only is cyber capability a quintessential element of national power, it has application in and influence over the diplomatic, informational, military, and economic arms of every state actor. Indeed, before the Allies can begin to address the challenges of cyberspace, they must first recognize their profound and far-reaching vulnerabilities in the cyber domain. NATO has already begun transforming its perspectives on cyber, unequivocally putting the "C" in DIME ("DIMEC"). In this regard, the Alliance is leading the endeavor to address the cyber challenges of a 21st century world order.

In light of Russia's alleged cyber attack campaign against Estonia in 2007, against Georgia in 2008, and against Ukraine since 2013, NATO's cyber warfare preparedness has become a prominent topic of interest. Evaluating the preparedness of the Alliance—namely, NATO's capability, readiness, and willingness to respond effectively to a cyber act of war—is essential to identifying areas of improvement for the largest defense organization in the world. If NATO failed to react effectively in a cyber or hybrid war

[6] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," August 24, 2016, https://www.csis.org/programs/strategic-technologies-program/cybersecurity/significant-cyber-incidents, 1, 3–5, 6–11, 13–14.

scenario,[7] it could weaken the Alliance in the eyes of its Allies and its adversaries. If NATO suffered losses during a cyberwarfare contingency, it would have to react to restore the security and integrity of the affected NATO area. For these reasons, the Alliance cannot afford to be unprepared for cyberwar.

C. EXPLANATIONS AND HYPOTHESES

As of 2016, a cyber attack has not brought a nation to war. NATO's Wales and Warsaw Summits affirmations nonetheless confirm that the Allies recognize that the potential exists for cyber aggression to trigger a kinetic war.[8] If an Ally experienced a major act of cyberwar, NATO may be more cybernetically than politically, economically, and militarily prepared to respond effectively. NATO's robust cyber strategy and extensive cooperative partnerships offset some of the organization's shortfalls in decision making, political resolve, crisis management readiness, and defense spending. NATO must continue its leadership role in the cybersecurity domain to meet evolving challenges resulting from technical and legal complexities, attribution difficulties, and the increasing diversity of cybernetic weapons.[9] If the Alliance wishes to remain ready and relevant in all security domains, it must advance its preparedness in the cyber one.

D. RESEARCH DESIGN AND METHODOLOGY

This thesis takes a qualitative approach to investigate NATO's level of preparedness to respond to an act of cyberwar against one or more of its Allies. The body of research analyzes policy papers, journal articles, the North Atlantic Treaty (frequently referred to as the Washington Treaty), defense reports, public poll surveys, and case studies. The thesis evaluates NATO's historical responses to the most recent geopolitically significant cyber attacks against NATO members and non-NATO countries. It also builds on current scholarship on NATO's cyber defense capabilities by

[7] Hybrid war is a military strategy that exploits multiple dimensions of warfare; hybrid tactics blend conventional military methods with unconventional forms of warfare that may include psychological or deception operations, cybernetic espionage and attacks, disinformation, and propaganda (Damien Van Puyveld, "Hybrid War—Does It Even Exist?" *NATO Review*, 2015, http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/, 1.)

[8] "Wales Summit Declaration," par. 72.

[9] Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 18–19.

assessing the cyber response policies, organizational evolution, cooperative partnerships, and decision-making protocols within the NATO framework. Since the study focuses on advances in cyber technology and policy, much of the research stems from the last five years. Additionally, the thesis evaluates public opinion trends and NATO's coalition performance to assess its readiness to conduct military operations if the collective defense principle (Article 5)[10] is invoked. Finally, the analysis examines economic data and policy white papers to evaluate spending patterns, defense commitments, and national security priorities to recommend relevant changes in policy and effort. The thesis reviews NATO's level of preparedness across seven key areas:

> **Cyber strategy.** The thesis assesses the quality of NATO's current cyber policy, doctrine, and standard operating procedures across three focal areas: comprehensiveness, execution, and clarity. It further evaluates the organization's structural and policy changes made in response to large-scale cyber attacks launched against NATO, its Allies, and its partners.
>
> **Cyber cooperation.** The thesis assesses the technical partnerships and level of cooperation among Alliance members and external agencies on cybersecurity matters.
>
> **Decision making.** The thesis studies NATO's institutional protocols to assess the organization's decision-making processes and procedures.
>
> **Political will.** The thesis reviews international surveys, political news articles, and the geopolitical context to ascertain the likelihood that public consensus within Alliance member states would support a collective defense response to a major act of cyberwar against an Ally.
>
> **Crisis management.** The thesis evaluates NATO's crisis management procedures, objectives, and operational performance during major combat operations to assess its crisis response effectiveness.
>
> **Defense spending.** The thesis evaluates national defense spending trends, cyber defense spending, and the economic readiness of five prominent NATO members—France, Germany, Italy, the UK, and the United States—in order to assess the Alliance's capacity to finance and sustain military operations if a cyberwar turned kinetic.

[10] Article 5 is the collective defense principle espoused in the Washington Treaty, which declares that an attack on one Ally is an attack on all of them; this principle of solidarity ensures that Alliance members will come together to assist in the mutual defense of one another in the case of an armed act of aggression (NATO, "Collective Defense—Article 5," March 22, 2016, http://www.nato.int/cps/en/natohq/topics_110496.htm, 1).

Defense policy prioritization. The thesis examines the national security and defense plans, objectives, and threat priorities of five leading NATO members—France, Germany, Italy, the UK, and the United States—in order to assess the Alliance's capacity and resolve to intervene militarily on behalf of an Ally first attacked in cyberspace.

The thesis employs a performance metric that ranks NATO's cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization in order to determine how ready the Alliance is to effectively address cyberwar threats to Euro-Atlantic security and stability. This metric of preparedness consists of the following three levels:

Minimal level of preparedness. This is the lowest level of preparedness. At this level, the Alliance would not meet minimum standards of readiness to effectively address, counter, and/or resolve an act of cyberwar against one or more of its members. Out of a numerical value ranking of 1–3, the Alliance would earn a score of 1.

Moderate level of preparedness. This represents an average or medium level of preparedness. At this level, the Alliance would meet the minimum standards of readiness to effectively address, counter, and/or resolve an act of cyberwar against one or more of its members. Out of a numerical value ranking of 1–3, the Alliance would earn a score of 2.

High level of preparedness. This is the highest level of preparedness. At this level, the Alliance would meet or exceed most standards of readiness to effectively address, counter, and/or resolve an act of cyberwar against one or more of its members. Out of a numerical value ranking of 1–3, the Alliance would earn a score of 3.

E. THESIS ORGANIZATION

The central elements of this thesis address NATO's overall preparedness to respond to a major act of cyber aggression against one or more of its members. The thesis is organized as follows: Chapter II provides a literature review concerning the most pertinent works related to the study. Chapter III offers an overview of cyber warfare and defense terminologies and describes the primary challenges, threats, and actors that NATO faces in cyberspace. Chapter IV discusses historical case studies of large-scale cyber attacks—past and ongoing—launched against NATO Allies and partners; it further considers NATO's political and organizational responsiveness in each of these cases.

Chapter V critically evaluates the strengths, weaknesses, and changes in the organization's level of preparedness to respond to a major act of cyberwar from a cybernetic, political, military, and economic perspective. It specifically assesses the Alliance in the areas of cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization. Chapter VI concludes the thesis and presents recommendations for policy and institutional improvement.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The topic of cyber defense has gained significant attention among governments, scholars, think tanks, industries, citizens, and international organizations. The rising interest in cyberspace shows in the vast collection of works available today on cyber warfare, defense, governance, and security. A reasonable subset of literature is devoted to the study of cyber and NATO—specifically, how NATO can develop and enhance its cyber capabilities and address virtual threats. Yet few studies critically examine the preparedness of the world's largest military Alliance to respond effectively to cyberwar. This thesis is intended to address this gap in the literature and to make a useful contribution to knowledge. The literature review evaluates eight pieces of scholarship, beginning with works that examine NATO's cyber capabilities and shortfalls.

A. HANNES KRAUSE

In a monograph titled "NATO on Its Way Towards a Comfort Zone in Cyber Defense," Hannes Krause offers an assessment of the progress made and the challenges encountered by NATO's cyber defense policies over the last few years. His report raises practical questions about Article 5 invocation—specifically the scope of the action that NATO should undertake to support an Ally attacked in the cyber domain.[11] He summarizes the Alliance's primary challenges as operational inflexibility, information sharing, and cyber interoperability.[12] He concludes with the following four recommendations: (1) that NATO act as an intermediary rather than as a provider of cyber assistance, (2) that NATO incorporate cyber in the defense planning process, (3) that NATO increase its transparency, and (4) that NATO integrate cyber scenarios into its military exercises.[13]

---

11 Hannes Krause, "NATO on Its Way Towards a Comfort Zone in Cyber Defense," *The Tallinn Papers*, no. 3, Cooperative Cyber Defense Center of Excellence, 2014, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_03.pdf, 2.

12 Krause, "NATO on Its Way," 3–4.

13 Krause, "NATO on Its Way," 3–5.

Krause presents valid findings. Indeed, the Alliance has already adopted to some extent many of his recommendations. Nonetheless, he does not discuss the potential negative consequences of cyber intelligence sharing among NATO members, which have varying levels of network security, cyber infrastructure, and national information assurance standards. While Krause never explicitly raises the question of NATO's readiness to counter an attack in the cyber realm, he does suggest that if NATO takes the four steps he prescribes, the organization will be closer to achieving its "cyber defense comfort zone."[14] One of the objectives of this thesis is to assess how far NATO has come with instituting improvements in its cyber capabilities, defenses, and policies.

B. REX HUGHES

Like Krause, Rex Hughes, who authored "NATO in Cyberspace: Digital Defenses," believes the Alliance has come a long way to address security problems in the electronic or "e" domain. While NATO has taken such milestone steps as creating the Cyber Defense Management Authority (CDMA) and opening the Cooperative Cyber Defense Center of Excellence (CCDCOE), the Alliance has made less progress in other areas.[15] Hughes asserts that NATO has not made demonstrable movement in formulating a global vision for cybersecurity and in advocating the enforcement of international legal standards regarding acts of cyberwar and cyberterrorism.[16] Since the writing of his article in 2009, however, NATO's CCDCOE has published the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, providing guiding principles for the conduct of nation states during cyberwar.[17] Yet, the legal conundrums surrounding cyber issues still persist, such as NATO's authority to conduct offensive cyber attacks or hack-back operations and the roles and responsibilities of prosecuting authorities under the Law of Armed Conflict, telecommunications regulations, and Article 51 of the United

14 Krause, "NATO on Its Way," 6.

15 Rex Hughes, "NATO in Cyberspace: Digital Defenses," *World Today*, 65, no. 4 (April 2009): 20.

16 Hughes, "NATO in Cyberspace," 20–21.

17 Jeffrey L. Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications* (Carlisle Barracks, PA: United States Army War College Press, 2014), 22.

Nations (UN) Charter.[18] Although NATO has taken critical strides in coordinating technical and legal policies in cyber defense, Hughes' article makes clear that there is still much for the Alliance to do in tackling the legal challenges of cyberspace.

C. NIKITAS NIKITAKOS AND PANOS MAVROPOULOS

In *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice,* edited by Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos, the authors explore the implications of information technology for policy, law, democracy, and national security.[19] In Chapter 10, Nikitas Nikitakos and Panos Mavropoulos discuss how cyber can both serve as an extension of a state's power and as a source of major vulnerability due to its unregulated, unprotected, and complex nature.[20] According to Nikitakos and Mavropoulos, cyberwar—like any war—is politically motivated; its ultimate objective is to compel the enemy to bend to one's will, sometimes by manipulating or weakening the public resolve of the adversary via attacks on critical infrastructure.[21] The authors' conclusions about cyberwar are applicable to this thesis because one must first comprehend why attackers strike in the cyber domain before assessing NATO's preparedness to thwart such attacks. One of the authors' conclusions about cyberwar is that it "is not coming…cyberwar has already arrived," which signifies that it is not a question of if a cyberwar could arrive on NATO's doorstep, but when.[22]

---

[18] Hughes, "NATO in Cyberspace," 21.

[19] Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos, ed. *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice* (New York: Springer, 2014), v.

[20] Nikitas Nikitakos and Panos Mavropoulos, "Cyberspace as a State's Element of Power" in *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice,* ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos (New York: Springer, 2014), 260.

[21] Nikitakos and Mavropoulos, "Cyberspace as a State's Element of Power," 266.

[22] Nikitakos and Mavropoulos, "Cyberspace as a State's Element of Power," 276.

D. PYTHAGORAS PETRATOS

In Chapter 11 of *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice*, Pythagoras Petratos delves into the cyber policies and institutions of NATO and the European Union (EU).[23] He finds that disparities among NATO and EU member states in cyber capability, technical infrastructure development, investment, and burden sharing have severely limited progress within the area of cyber governance.[24] He pertinently questions the EU's capacity to lead and sustain military operations on a significant scale while maintaining the security and control of its internal cyber networks.[25] This thesis applies to NATO the operational queries that Petratos raises about the EU in order to investigate the Alliance's military preparedness for cyberwar. If cyber aggression turns kinetic, does the Alliance have the capability, capacity, and will to sustain its engagement in the conventional warfighting domain and prevail? The thesis endeavors to answer this question. While the thesis disagrees with Petratos's assertion regarding the possibility of a cyber arms race between the United States and the EU, it concurs that the cyber innovation and investment divide between the United States and its European Allies has led to "free rider" problems in NATO.[26] In the same way that Petratos considers whether the EU invests sufficiently in its information and communications technology (ICT) infrastructure,[27] this thesis evaluates some of NATO's ICT budgets. Petratos concludes that the EU must increase its spending and enhance its cooperation with the public sector, private industry, and NATO, which is in line with current mainstream thinking.[28]

---

23 Pythagoras Petratos, "Cybersecurity in Europe: Cooperation and Investment" in *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice*, ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos (New York: Springer, 2014), 278.

24 Petratos, "Cybersecurity in Europe: Cooperation and Investment," 278.

25 Petratos, "Cybersecurity in Europe: Cooperation and Investment," 289.

26 Petratos, "Cybersecurity in Europe: Cooperation and Investment," 296.

27 Petratos, "Cybersecurity in Europe: Cooperation and Investment," 297.

28 Petratos, "Cybersecurity in Europe: Cooperation and Investment," 298.

E. MARIOS PANAGIOTIS EFTHYMIOPOULOS

In Chapter 12 of *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice,* Marios Panagiotis Efthymiopoulos discusses NATO's Smart Defense policy as it relates to the Alliance's cyber defense strategy. He holds that NATO is "well prepared" for "current and future challenges" in cyber, arguing that the Alliance should continue to innovate, evolve, and enhance its policies and methods.[29] The chapter concludes with proposals that are similar to those advanced by Krause—above all, greater information sharing.[30] Efthymiopoulos also proposes changes that deviate from the mainstream, including but not limited to the establishment of a NATO Center of Excellence for Electronic Warfare (EW), joint-level military cooperation in EW, and budgets structured around cyber requirements as defined by the Smart Defense paradigm.[31] While some of these proposals are noteworthy, a few fail to address the consequences of—and strategic obstacles to—multinational information sharing within the highly sensitive domain of electronic warfare.

F. FRANKLIN D. KRAMER

In "Achieving International Cyber Stability," Franklin D. Kramer delves into the role that cyber could play in modern warfare and the detrimental effects that cyberspace could have on critical infrastructure; he also evaluates how NATO and other international organizations, including the EU, could help achieve overall stability in cyberspace to prevent cyber incidents from escalating into geopolitical conflicts.[32] Likewise, Kramer underscores the critical role that resiliency, transparency, and cooperation play in the cybernetic domain and recommends cyber norms that complement many of the guidelines

---

[29] Marios Panagiotis Efthymiopoulos, "NATO's Cyber-Defense: A Methodology for Smart Defense" in *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice*, ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos (New York: Springer, 2014), 305–306.

[30] Efthymiopoulos, "NATO's Cyber-Defense," 316.

[31] Efthymiopoulos, "NATO's Cyber-Defense," 316.

[32] Franklin D. Kramer, "Achieving International Cyber Stability," Atlantic Council, (2012), http://www.atlanticcouncil.org/images/files/publication_pdfs/403/kramer_cyber_final.pdf, 1.

in the *Tallinn Manual*.[33] In addition to other proposals, he submits that nations should take steps to upgrade hardware and software capabilities, engage with Internet service providers on potential network threats, establish a Cyber Stability Board with likeminded governments and private sector actors, and cooperate transparently with partners and adversaries on common cybersecurity issues.[34] Kramer's proposed initiatives and operational approaches to cyber stability make his work an invaluable contribution to the cyber policy debate.[35]

G. JASON HEALEY AND LEENDERT VAN BOCHOVEN

In "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO," Jason Healey and Leendert van Bochoven contend that NATO should develop an advanced cyber distant early warning monitoring system to afford decision-makers adequate time to address major cyber incidents.[36] Healey and van Bochoven make practical proposals, such as encouraging the Alliance to depend more on the private sector for early warning intelligence, since private industry maintains the best resources, processes, and indications and warning systems already in place.[37] Additionally, Healey and van Bochoven advocate the Alliance engage with civilian and military computer emergency response teams (CERT) and expand the intelligence capability of NATO's Cyber Threat Analysis Cell (CTAC).[38] By focusing on strategic cyber attacks and incorporating the abovementioned solutions into a cyber phased adaptive approach modelled after the European Phased Adaptive Approach in the U.S. Ballistic Missile Defense program, NATO can credibly prepare for large-scale cyber incidents without significant pain or cost.[39]

---

33 Kramer, "Achieving International Cyber Stability," 1.

34 Kramer, "Achieving International Cyber Stability," 2, 8.

35 Kramer, "Achieving International Cyber Stability," 6, 10, 12.

36 Jason Healey and Leendert van Bochoven, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO," Atlantic Council (2012), Washington, DC: The Atlantic Council of the United States, http://www.atlanticcouncil.org/images/files/publication_pdfs/403/NATO%20Cyber%20Warning%202012.pdf., 1.

37 Healey and van Bochoven, "Strategic Cyber Early Warning," 1, 7.

38 Healey and van Bochoven, "Strategic Cyber Early Warning," 7.

39 Healey and van Bochoven, "Strategic Cyber Early Warning," 7.

The authors present a credible argument, asserting that NATO must prioritize strategic-level cyber attacks that could trigger Article 4[40] or Article 5 of the North Atlantic Treaty above everyday tactical-level cyber attacks.[41] Although Healey and van Bochoven wrote their paper in 2012, their recommendations still have merit for this thesis. A significant component of this study is to assess NATO's cyber response preparedness, which is dependent upon the organization's ability to anticipate, detect, and resolve network intrusions before they rise to the level of an Article 5 response.

H. JASON HEALEY AND KLARA TOTHOVA JORDAN

Jason Healey and Klara Tothova Jordan in "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" offer one of the most succinct and yet thorough reports on NATO's progress in developing its cyber vision, capabilities, and policies. Healey and Jordan provide a timeline of the Alliance's cyber milestones, discussing in detail the establishment of the 2002 Cyber Defense Program, the NATO Computer Incident Response Capability (NCIRC), the 2008 NATO Cyber Defense Policy, the Cyber Defense Management Board, the Cyber Defense Committee, and the 2014 Enhanced NATO Policy on Cyber Defense.[42] Healey and Jordan emphasize that NATO has done more than just alter its institutions and policies—it has changed its mindset and awakened to the realities of its e-security environment.[43] The report offers practical solutions to the cyber problems facing the Alliance, advocating robust coordination with the European Union Agency for Network and Information Security (ENISA), especially through involvement in NATO exercises.[44] Healey and van Bochoven also propose that

---

[40] Article 4 is the principle of consultation espoused in the Washington Treaty; it affords NATO member states the opportunity to meet, consult, and voice official opinions on an issue before any formal decision or action is taken on its behalf. (NATO, "The Consultation Process and Article 4," March 17, 2016, http://www.nato.int/cps/en/natohq/topics_49187.htm, 1).

[41] Healey and van Bochoven, "Strategic Cyber Early Warning," 1–2, 5.

[42] Jason Healey and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Atlantic Council, September 2014, http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf, 1–5.

[43] Healey and Jordan, "NATO's Cyber Capabilities," 2, 7.

[44] Healey and Jordan, "NATO's Cyber Capabilities," 6.

the Alliance consider offensive coordination efforts that do not divulge sensitive information on national cyber capabilities.[45]

While much of the literature on NATO's cyber capabilities reiterates the need for greater information sharing, Healey and Jordan go beyond this. They suggest that NATO foster relationships with cyber institutions in the private sector and build cyber crisis coordination cells outside of Rapid Reaction Teams (RRT) that employ technical experts and military leadership alike.[46] While the authors contend that an Article 4 or Article 5 response resulting from a cyber attack is likely to occur during an ongoing geopolitical conflict, it is also possible that a major cyber attack could precede or trigger a crisis.[47] Overall, the article by Healey and Jordan is rich in information regarding NATO's past, present, and future in cyberspace and is consistent with most mainstream analyses about NATO's cyber readiness and the way forward.

I. JAMIE SHEA

In his article titled "NATO: The Challenges Ahead," Jamie Shea, NATO's Deputy Assistant Secretary General for Emerging Security Challenges, evaluates the current strategic security issues confronting the Alliance, such as transnational terrorism and a resurgent Russia.[48] He discusses cyber in conjunction with the hybrid warfare debate, attempting to determine how NATO—an organization that traditionally operates reactively based on hard intelligence and thorough deliberation—can adapt to respond proactively and decisively based on ambiguous and fragmentary information.[49] He proposes NATO reforms that address budgetary inefficiencies and nominal coordination efforts with the EU.[50] In addition, he goes beyond the scope of the proposals made by some of his contemporaries by addressing the need for NATO to develop partnerships

45 Healey and Jordan, "NATO's Cyber Capabilities," 6.

46 Healey and Jordan, "NATO's Cyber Capabilities," 7.

47 Healey and Jordan, "NATO's Cyber Capabilities," 7.

48 Jamie Shea, "NATO: The Challenges Ahead," *Global Affairs* (2015), http://www.tandfonline.com/doi/full/10.1080/23340460.2015.979542, 6.

49 Shea, "NATO: The Challenges Ahead," 2.

50 Shea, "NATO: The Challenges Ahead," 2, 6.

with supply chain management firms and leverage the intelligence services provided by its Allies.[51] Shea also addresses the need for NATO's Readiness Action Plan to be flexible for the long-term and adequately address evolving geopolitical realities.[52] Finally, he discusses strategic messaging—a key area rarely mentioned in the typical NATO cyber texts. He astutely observes that for NATO to gain the budgetary support necessary for national defense plans and the public's support for its security operations, the Alliance must educate the Allied publics on its missions and policies.[53] In all, Shea provides a concise summary and perceptive analysis of the most pressing issues currently facing the Alliance. His article has informed this study of the political and strategic deficits affecting the organization's readiness for cyberwar.

J. KEN M. JONES

The March 2015 thesis by Ken M. Jones investigates some issues comparable to those examined in this thesis. In "Cyberwar—The Next Frontier for NATO," Jones analyzes three main areas: (1) NATO's response readiness for cyber aggression directed against a member state, (2) the nature and scope of this response, and (3) the preconditions for an invocation of Article 5.[54] He discusses the contributions the *Tallinn Manual* has made toward the establishment of legal and behavioral standards, which national governments—especially those of Allied member states—can employ to address cyber attacks.[55] There is a minor historical inaccuracy when Jones states that the 2007 cyber attacks against Estonia were brought under control after "several days,"[56] when in actuality the attacks persisted for three weeks.[57]

---

[51] Shea, "NATO: The Challenges Ahead," 2–3.

[52] Shea, "NATO: The Challenges Ahead," 4.

[53] Shea, "NATO: The Challenges Ahead," 5.

[54] Ken M. Jones, "Cyberwar—The Next Frontier for NATO" (master's thesis, Naval Postgraduate School, 2015), 1, 3.

[55] Jones, "Cyberwar," 19–25.

[56] Jones, "Cyberwar," 32.

[57] Ian Traynor. "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, May 16, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia, 1.

Jones also presents an analysis of the conditions that led to NATO's unprecedented Article 5 invocation—the September 11, 2001 attacks—and applies this institutional reasoning to conceive of situations that may warrant another call for collective defense.[58] After critically analyzing the Alliance's Cyber Defense Policy and e-capabilities,[59] Jones assesses that it is difficult to determine NATO's readiness for cyber attacks that fall outside of its policies and procedures.[60] Jones adds that the conditions necessary to trigger Article 5 depend on the severity of the cyber attack and the Alliance's attribution success.[61] He acknowledges that NATO's ambiguity affords it flexibility, allowing the organization to respond in a myriad of ways, including kinetically, economically, and diplomatically.[62] He concludes with several recommendations, the first reinforcing an argument originally raised by Healey and van Bochoven, who proposed the development of a cyber distant early warning system.[63] Jones goes further in recommending that the Alliance's cyber strategy focus on deterrence by denial techniques.[64] In addition, he recommends that NATO maintain its strategic ambiguity on Article 5 thresholds while increasing the level of information sharing among Alliance members.[65] He also advocates that NATO create a multinational team of computer forensic and hacking experts to enhance the resiliency and robustness of its digital networks.[66]

Overall, Jones' thesis assesses the Alliance's readiness to respond to a major cyber attack from a purely technical standpoint. It does not evaluate NATO's readiness from a multidimensional optic in which political, military, economic, and decision-making factors are weighed and considered—a gap in the body of knowledge that this

58 Jones, "Cyberwar," 25–26.

59 Jones, "Cyberwar," 35.

60 Jones, "Cyberwar," 36.

61 Jones, "Cyberwar," 37–38.

62 Jones, "Cyberwar," 40.

63 Jones, "Cyberwar," 40.

64 Jones, "Cyberwar," 45–46.

65 Jones, "Cyberwar," 45–47.

66 Jones, "Cyberwar," 47.

thesis hopes to address. This thesis expands on the current literature by analyzing NATO's capabilities, shortfalls, strengths, and weaknesses across several key areas, including cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization. Each of these dimensions affects NATO's level of preparedness to respond effectively in the face of cyber aggression.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NATO AND CYBERSPACE

Scholars and experts within NATO, national governments, private industry, and academic think tanks debate how to best address the challenges associated with cyber, which include attribution difficulties, law enforcement limitations, private and governmental responsibilities, and conflict de-escalation considerations.[67] Over the years, the Alliance has taken actions to improve its capacity to address cybernetic threats. In 2010, the Alliance published the Strategic Concept, which provided NATO's vision and priorities for security across Europe and the Euro-Atlantic region and defined the organization's three essential core tasks as cooperative security, crisis management, and collective defense.[68] While the Alliance touched upon general cybersecurity issues in the Strategic Concept, it put the spotlight on cybersecurity at the Wales Summit four years later.[69] On September 5, 2014, NATO made a clear and unprecedented declaration of its stance in the international cyber debate.

At the 2014 Wales Summit, NATO heads of state and government publicly acknowledged the growing geopolitical significance of cyber defense and made three critical announcements in this regard. First, the Alliance affirmed that cyber defense would become part of its collective defense, as defined in the Strategic Concept.[70] Second, NATO declared it would apply international law in the cyber realm.[71] Third, NATO vowed that it would consider a cyber attack that met the threshold of a conventional armed attack an act of war, which could trigger a collective defense response under Article 5 of the Washington Treaty.[72]

---

67 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 18–19.

68 "Improving NATO Capabilities," NATO, February 16, 2015, http://www.nato.int/cps/en/natohq/topics_49137.htm, 1.

69 *Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization*, NATO, 2010, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, 11, 16.

70 "Wales Summit Declaration," par. 72.

71 "Wales Summit Declaration," par. 72.

72 "Wales Summit Declaration," par. 72.

On July 9, 2016, at the Warsaw Summit, NATO made another series of public affirmations regarding its commitment to Allied cyber defense and to supporting global security and stability in cyberspace.[73] NATO unveiled its Cyber Defense Pledge, under which it agreed to strengthen the cybersecurity standards and resiliency of its national networks in accordance with the Enhanced Policy on Cyber Defense.[74] In recognition of the growing need for enhanced partnerships, NATO affirmed it would deepen its cooperation with the EU, partner nations, industry, and academic institutions through Technical Arrangements and the NATO Industry Cyber Partnership.[75] Finally, according to its official communiqué, the Alliance plans to complement these policy and cybernetic efforts by incorporating cyber defense more fully into its operational planning, exercises, and missions.[76]

A. DEFINITIONS

In the physical world, the destruction of national assets, damage to critical infrastructure, and civilian casualties bring to mind acts of war. The attacks of September against the Pentagon and the Twin Towers, the 1964 attack against the USS *Maddox* in the Tonkin Gulf, and the 1941 attack against Pearl Harbor all show what acts of war look and feel like. In the cyber domain, however, an act of aggression is less palpable and more ambiguous, and thus it may bear multiple definitions.

1. Cyber Attack

According to the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, a cyber attack is a defensive or offensive cyber operation that could reasonably cause injury, death, damage, or destruction to persons or objects.[77] Owens, Dam, and Lin define cyber attacks as "deliberate actions to alter, disrupt, deceive, degrade, or destroy

---

73 "Warsaw Summit Communiqué," NATO, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm., par. 70.

74 "Warsaw Summit Communiqué," par. 71.

75 "Warsaw Summit Communiqué," par. 71.

76 "Warsaw Summit Communiqué," par. 70.

77 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare,* (New York: Cambridge University Press, 2013), 106.

computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[78] Borrowing from and expanding on the language in these two definitions, this thesis defines a cyber attack as a deliberate defensive or offensive cyber operation that causes or could cause harm or destruction to persons, objects, infrastructure, networks, systems, and/or programs.

2. Cyber Incident

In cyberspace, non-violent cyber operations that seek to obtain, manipulate, or exploit information are forms of cyber espionage and cyber exploitation that are different from cyber attacks but are frequently confused with them.[79] Cyber attacks as well as espionage, exploitation, and hacking attempts in cyberspace are all forms of cyber incidents.

3. Cyberwar

An act of cyberwar is on a more complex scale than a cyber attack. Alison Lawlor Russell defines cyberwar as "a state of hostilities between countries or their agents (including organized non-state groups under the control of the state) that involves cyber operations that result in damage, destruction, or death."[80] These cyber hostilities may involve a constant exchange of cyber attacks and cyber incidents that could escalate into an armed attack in the sense of Article 5 of the Washington Treaty. NATO's preparedness to respond to such a major act of cyberwar is the focus of this thesis.

4. An Act of War

The U.S. Code defines an act of war as the following: "any act occurring in the course of—(A) declared war, (B) armed conflict, whether or not war has been declared, between two or more nations, or (C) armed conflict between military forces of any

---

[78] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, ed., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 1.

[79] Schmitt, *Tallinn Manual*, 106.

[80] Russell, *Cyber Blockades*, 8.

origin."[81] In 2012, Harold Koh, then the legal advisor to the U.S. State Department, declared that cyber attacks that "result in death, injury, or significant destruction would likely be viewed as a use of force….[and] would constitute a use of force."[82] Thus, this thesis defines "a major act of cyberwar" as a cyber act that effects damage comparable to that of an armed attack, including loss of life and destruction of critical infrastructure, which rises to the level of an act of war. For NATO, crossing this line in cyberspace could be the trigger for a kinetic or cybernetic response under Article 5.

B. CYBER FACTORS AFFECTING AN ARTICLE 5 DECLARATION

Cyberwar has emerged as one of the most efficient means to expose vulnerabilities and effect destruction against organizations, industries, and nations. Frequent and severe cyber attacks against NATO members, including Estonia, France, Germany, the UK, and the United States, have shown the pervasiveness of these challenges.[83] If the Alliance was confronted with a major act of cyberwar, multiple variables would influence NATO's decision making. Geopolitical considerations notwithstanding, a decision by the Alliance to invoke Article 5 in response to a major act of cyberwar could depend on four main factors: (1) the type of threat, (2) the threat severity, (3) attribution sensitivities, and (4) the identity of the cyber attacker.

1. Types of Threats

Many of the challenges that cyberspace poses to NATO derive from the very classification of the cyber threat. Since the cyber dimension offers many ways for hackers to disrupt, degrade, harm, and attack, cyber incidents generally fall into various categories. Some experts in the cyber field classify cyber incidents and attacks according to integrity, availability, and confidentiality.[84] Cyber attacks that compromise the integrity of an organization's networks or data do so for the purposes of propaganda,

---

[81] "18 U.S. Code § 2331—Definitions," Cornell University Law School, accessed August 1, 2016, https://www.law.cornell.edu/uscode/text/18/2331, 1.

[82] Koh quoted in David S. Yost, *NATO's Balancing Act* (Washington, DC: United States Institute of Peace Press, 2014), 44.

[83] "Significant Cyber Incidents since 2006."

[84] Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 15.

disinformation, coercion, intimidation, or destruction.[85] In 2014, North Korea's hacking of Sony Pictures Entertainment employed this method of cyber blackmail—threatening destructive actions—in an attempt to block the release of a movie depicting the assassination of Kim Jong Un. Conversely, cyber attacks that disrupt the availability of websites and intranets are intended to prevent the public from accessing data resources and services, such as transportation, banking, and emergency support.[86] The distributed denial-of-service (DDoS)[87] cyber attacks that brought down parliamentary, banking, and media websites in Estonia in 2007 constitute a prime example of this type of threat.[88] Finally, cyber incidents that violate confidentiality target information for the purposes of fraud, data mining, identity and personal data theft, blackmail, and/or espionage.[89] China's reported 2015 electronic espionage attack on the Office of Personnel Management (OPM) that stole sensitive and classified information on 22 million U.S. government, contractor, and military personnel exemplifies this type of data breach.[90] While these types of incidents represented significant network intrusions against Allied member states, they did not trigger a collective response from NATO, in part due to their level of severity.

2. Threat Severity Levels

The severity of a cyber attack across the integrity, availability, and confidentiality domains directly affects the level of response. Although cyber incidents within the

---

85 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 15.

86 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 15.

87 Distributed denial-of-service (DDoS) attacks are cyber strikes that overwhelm a computer system by sending continuous requests for information to the targeted system's routers and/or servers, causing the system to shut down; hackers typically carry out DDoS attacks by hacking into computers from multiple locations and repurposing them for malicious intent without the computer owner's knowledge. Once these computers are compromised by hackers, they are known as botnets or "zombie" computers. (Radziwill, Yaroslav, *Cyber Attacks and the Exploitable Imperfections of International Law*, (Boston: Brill-Nijhoff, 2015), xiv, 328).

88 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 26.

89 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 15.

90 Ellen Nakashima, "Chinese Government has Arrested Hackers it says Breached OPM Database," *The Washington Post*, December 2, 2015, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html, 1.

confidentiality domain are more frequent than attacks in the other two domains, information breaches—no matter the scale—have yet to trigger an armed conflict. While cyber espionage and other violations in confidentiality can become grave threats to national security, these activities—though prosecutable crimes—do not represent in and of themselves acts of war. This is partially due to the pervasive understanding that all countries spy on each other whether friend or foe. Another major factor derives from the guidance articulated under Article 51 of the UN Charter, which states that a member state has "the inherent right of individual or collective self-defense" if an armed attack occurs.[91] Espionage alone does not meet the requirements of an armed attack.

While some may argue that a nation's discovery of a particular data breach (such as that of its nuclear codes) could characterize an imminent existential threat and warrant a preemptive strike, cyber attacks against confidentiality have yet to trigger an armed preemptive response. If an aggressor state obtained critical information through cyber espionage, which facilitated an armed attack, the aggressor state's armed attack alone would justify the targeted state's resort to self-defense—not the preceding data breach. Many nations choose to handle violations of cyber confidentiality through non-military means such as diplomacy, legal prosecution, cyber retaliation, or economic sanctions.

Contrary to electronic attacks on confidentiality, cyber activities that violate integrity and availability—like the distributed denial-of-service attacks against Estonia in 2007—have the potential to trigger an armed conflict. According to Harold Koh, then the legal advisor to the U.S. State Department, "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force."[92] Severe cyber attacks that disrupt the availability of power, water, transportation, and financial services could effectively shut down a country. Thus, cyber acts of war could include information, power, and network disruptions that cause the destruction of critical infrastructure and loss of life.[93] At the 2014 Wales Summit, NATO stood behind this judgment when it

91 Yost, *NATO's Balancing Act,* 248.

92 Yost, *NATO's Balancing Act,* 44.

93 Yost, *NATO's Balancing Act,* 44.

declared that it would reserve the right to invoke Article 5 if a cyber attack reached the magnitude of a conventional attack on one of its members.[94] The type and severity of the cyber attack would factor heavily in NATO's political calculus to determine its appropriate response.

The distributed denial-of-service (DDoS) attacks that struck Estonia in 2007 and Georgia in 2008 show two high-profile cases in which availability and integrity attacks created social disturbances and political instability but did not rise to the level of an armed attack.[95] In Estonia, hacktivists[96] targeted media and parliamentary websites and took down financial services, producing inconveniences and hardships for the technologically reliant population.[97] Cyber attacks against Georgian websites disrupted the dissemination of government information throughout the Georgia-Russia conflict.[98] While the cyber attacks against Georgia generated strategic-level effects, they were less pervasive than those against Estonia because Georgia's economy and government were not as Internet dependent.[99] If a state actor orchestrated such attacks against an Alliance member today and legal attribution was known, the attacks could possibly constitute an act of war. Nonetheless, if it was in the security interests of the Alliance, NATO could choose to respond even if a cyber attack did not rise to the perceived threshold of a conventional attack. Throughout all these cases, the type and severity level of the act of cyber aggression would factor heavily into the decision making calculus of NATO and the Ally attacked.[100] Still, attribution sensitivities can oftentimes serve as the most significant priority in determining an appropriate response.

---

94 "Wales Summit Declaration," par. 72.

95 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 26, 28.

96 In this thesis, the term "hacktivists" refers to individuals who engage in political activism by using cyberspace as their primary tool. Some hacktivists act on their own initiative in support of their own agendas, but others are funded by governments. The activities of hacktivists offer governments an option for "plausible deniability." (Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 14, 28).

97 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 26.

98 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 28.

99 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 28.

100 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 15, 24–26.

3. Attribution

Cyberspace facilitates a certain expectation of anonymity.[101] Identifying a perpetrator can be difficult in any criminal case, but when an offense is committed in the cyber dimension, the challenges are magnified. Accurately determining the identity of an attacker and proving culpability can be impractical using cyber tools.[102] Often times, cyber criminals can disguise their involvement and conceal their identities through proxies. A state may know who was behind a penetration of its government network, but may not want to publicize this knowledge for fear of relinquishing a particular classified cyber detection capability. Indeed, cyber weapons are only effective as long as they remain a secret.[103] Since a nation could lose more than it hopes to gain by publicly attributing a cyber attack to another entity, some may choose to forego making an attribution finding public.[104]

Even if the source of an Internet Protocol (IP) address is obtained accurately, the borderless nature of the Internet can complicate establishing legal culpability. For example, if a website that contains malware is owned in China but has a Polish address and a Danish host, holding the proper party accountable becomes a daunting challenge.[105] Aside from legal complications, the protracted length of time required to ascertain the true identity of a cybercriminal can corrode the credibility and legitimacy of attribution on the political stage and hinder the prosecution of the guilty parties.

Nonetheless, attribution of any crime is a prerequisite to formal action. To legitimize a response of collective defense, NATO would have to attribute and in some way show how it identified the culprit behind the act of cyberwar, which targeted one or more of its members; failure to do so would impede an Allied response. If NATO or an Ally was able to publicly attribute a cyber attack without a compromise of its cybernetic

---

101 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 24.

102 Nikitakos and Mavropoulos, "Cyberspace as a State's Element of Power," 271.

103 Ravi R. Hichkad and Christopher J. Bowie, "Secret Weapons & Cyberwar," Armed Forces Journal, (2012), http://www.armedforcesjournal.com/secret-weapons-cyberwar-2/, 1.

104 Martin C. Libicki, "Brandishing Cyber Capabilities," RAND National Defense Research Institute (2013), http://www.rand.org/pubs/research_reports/RR175.html, 13.

105 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 23.

capabilities, then an Article 5 response might be likely. Much would also depend, however, on the type of cyber aggression launched, the severity of the cyber attack, and the identity of the cyber actor.

4. Cyber State and Non-State Actors

The perpetrators of cybercrime and cyber terrorism come in many forms. Non-state actors, including spyware and malware authors, spammers, phishers, disgruntled insiders, botnet operators, and other black-hat hackers may initiate cyber attacks at an individual or small-unit scale.[106] States and corporations can operate with organized crime factions and militias to perform sabotage or industrial espionage—the collection of a corporation's intellectual, personnel, and/or proprietary information for commercial and/or political ends.[107] Hacktivists, like the alleged perpetrators in the cyber attacks against Estonia and Georgia in 2007 and 2008, respectively, initiate cyber campaigns against corporations and state actors typically for political, ideological, or financial purposes.[108] Terrorists use cyber methods to fight asymmetrically against stronger state actors to damage a nation's critical infrastructure, harm its citizens, and shake public confidence.[109]

This thesis assesses the prospects for terrorist and state actors to provoke an Article 5 declaration due to the high probability that it would take a major act of cyberwar by one of these two types of aggressors to elicit a collective and forceful response from the Alliance.

Although state and non-state actors commit millions of cyber attacks against NATO and its members every day, most of these acts have not provoked and would not elicit an official collective reaction.[110] Even when NATO's own networks have been hacked, the Alliance has historically not responded with force. In 2012, when Anders

---

106 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 14.

107 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 14.

108 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 14.

109 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 14.

110 "Significant Cyber Incidents since 2006," 3, 5, 7–9.

Fogh Rasmussen, then the Secretary General, stated that NATO had experienced "over 2500 'significant cases' of cyber attacks on its systems," none of them triggered an official collective response.[111] In 2014, NATO's Wales Summit Declaration showed a shift in organizational mindset. NATO declared for the first time in its history that it would reserve the right to invoke Article 5 in the event of a major cyber attack that reached the magnitude of a conventional attack on one of its members.[112] Although NATO would normally respond to small-scale attacks through defensive technical means or through the deployment of a Rapid Reaction Team (RRT) or unit from the NATO Communications and Information Systems (CIS) Group, there is a high probability that it would take a major state-sponsored or terrorist act of cyber aggression to provoke an Article 5 response—a response that would be tailored to the contingency and different for each actor.[113]

a. Scenario One: Terrorist Actor

If a terrorist organization attacked an Ally in cyberspace at the severity level of an armed attack, NATO would respond appropriately. For example, if the Islamic State of Iraq and the Levant (ISIL) engineered a distributed denial-of-service (DDoS) attack against a NATO member that caused severe damage to national power grids, contamination of public water supplies, paralysis of government web services, and/or loss of life, there is a high probability that the Allied member would invoke Article 4 for consultations with its Allies. The North Atlantic Council (NAC) would likely vote either to deploy a Rapid Reaction Team (RRT) without an Article 5 invocation or approve an Article 5 response that might include a mixture of military support and cyber defensive solutions, including RRT deployment. The Alliance could seek a UN Security Council Resolution to secure legitimacy for its efforts—like it did after the September attacks;

111 Yost, *NATO's Balancing Act*, 47.

112 "Wales Summit Declaration," par. 72.

113 "Men in Black—NATO's Cybermen," NATO, April 24, 2015, http://www.nato.int/cps/en/natohq/news_118855.htm, 4; Healey and Jordan, "NATO's Cyber Capabilities," 6; "Defending the Networks: The NATO Policy on Cyber Defense," NATO, 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf, 1–3.

however, if it failed to obtain such a resolution, NATO could still decide to engage with force—on the basis of Article 51 of the UN Charter.[114]

NATO has shown its resolve before in the face of a terrorist organization—namely Al Qaeda—which was the only time in its history it invoked Article 5.[115] The Alliance would likely capitalize on the opportunity to display its solidarity, resolve, and combined military prowess, especially within the current strategic environment in which revisionist powers such as China, Iran, and Russia consistently try to rebalance against the United States and NATO. What could be a louder deterrent to NATO's adversaries than a vigorous and collective response against an aggressive terrorist organization?

b. Scenario Two: State Actor

In a just society, whenever a crime is committed and the identity of the perpetrator is known, the offender's identity has no bearing on the legal outcome—unless that perpetrator possesses a nuclear arsenal. For NATO, any action that could escalate to a nuclear conflict would be taken with extreme caution.[116] If NATO wants to maintain and enhance the credibility of its cyber deterrent, however, it cannot rule out physical retaliation against nuclear-armed states.

In theory, it would take only one Ally, nervous about an impending nuclear war in its backyard, to block consensus during a vote in the NAC. In this way, NATO's consensus rule could in some circumstances impede a collective action involving all the Allies against a nuclear-armed actor in response to its state-sponsored cyber aggression. Nevertheless, even if some Allies blocked consensus in the NAC, the other Allies could take action under Article 51 of the UN Charter. It should be noted that during the Cold War, individual Allies—notably the United States—made strategic overtures to suggest it

---

[114] Leo Michel, "NATO Decision Making: Au Revoir to the Consensus Rule?" *Strategic Forum*, no. 202 (2003), Institute for National Strategic Studies National Defense University, https://www.ciaonet.org/attachments/12787/uploads, 2.

[115] Michel, "NATO Decision Making," 3.

[116] David S. Yost, "The U.S. Debate on NATO Nuclear Deterrence," *International Affairs* 87, no. 6 (2011): 1405.

would not rule out unilateral actions to safeguard its own national interests.[117] In fact, according to Naval Postgraduate School professor David Yost, "The United States enhanced the credibility of its extended deterrence commitments, despite its vulnerability to Soviet nuclear attack, by making clear to Moscow that it regarded its own national security interests as being at stake along with those of its Allies."[118]

In summary, no one can predict whether or how NATO will respond to a major act of cyber aggression directed against one or more of the Allies. Even if a cyber incident rises to the level of an armed attack and NATO has the political grounds and attributive evidence it needs to engage, this does not necessarily mean that NATO will respond collectively or with force. Political cohesion issues can arise in the face of any type of attack.

In the past, NATO's decisions not to respond with force have derived from difficulties and sensitivities with attribution. Divulging attributive evidence could expose certain advanced cybernetic capabilities to adversaries and possibly open the Alliance to further attacks. The Alliance's abstention from a forceful collective response has also rested in part on judgments regarding the type and level of severity of network attacks. Finally, another factor has been NATO's historic reliance on deterrence and cyber defense principles instead of offensive strategies. Although a NATO response to a major act of cyberwar will depend on the geopolitics of each case, Article 5 invocation is most likely when the following four conditions are all present: (1) the cyber attack occurs in the integrity and/or availability domains, (2) the severity of the cyber aggression meets the threshold of an armed attack, (3) attribution can be obtained without a compromise of cybernetic capability, and (4) the cyber aggression is sponsored by a state actor or terrorist organization.

[117] Yost, "U.S. Debate on NATO Nuclear Deterrence," 1405.

[118] Yost, "U.S. Debate on NATO Nuclear Deterrence," 1405.

IV. CYBER CASE STUDIES: CYBER ATTACKS AGAINST NATO ALLIES AND PARTNERS

This chapter explores NATO's responses to unprecedented global cyber aggression launched against three countries—one a NATO Ally and two NATO partners.

A. CYBER ATTACKS AGAINST A NATO ALLY

Cyber attacks occur every day against NATO Allies, including France, Germany, Italy, the UK, and the United States. One of the most severe acts of cyber aggression occurred against one of the Alliance's newest members—Estonia.

1. Estonia

In April 2007, Estonia was struck by the largest campaign of cyber attacks on record after the government removed a Soviet war memorial statue, the Bronze Soldier, from the city center to the less prominent Tallinn Military Cemetery.[119] The action was evidently a political attempt to "de-Russify" part of the country's public space and/or reduce Russia's cultural influence within the Baltic state.[120] Estonia's Russian minority community, which then comprised 26 percent of the population, perceived the government's action as an affront to Russian identity, culture, and history.[121] The decision precipitated nationalist demonstrations by the Russian-speaking populace inside the country.[122] While the Estonian government may have foreseen public dissention as a logical byproduct of its actions, the type of domestic backlash that followed on April 26, 2007 was completely unanticipated.

What began as street riots transitioned to three weeks of coordinated distributed denial-of-service (DDoS) cyber attacks on parliamentary, banking, university, and media

119 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss, 49–50.

120 Herzog, "Revisiting the Estonian Cyber Attacks," 50.

121 Herzog, "Revisiting the Estonian Cyber Attacks," 49.

122 Herzog, "Revisiting the Estonian Cyber Attacks," 50.

websites.[123] The DDoS tactics strained network servers, blocking Estonian users' access to countless websites.[124] Russian hacktivists and sympathizers attacked Estonia's electronic infrastructure via thousands of botnets or "zombie" computers (located in 50 countries around the globe), whose security had been hacked and secretly repurposed for malicious employment.[125] The cyber attacks—which were coordinated through Russian language chat rooms and weblogs— left Estonians without access to not only key websites but also to their money; credit and debit cards became virtually useless.[126]

As one of the most electronically interconnected nations on the planet, Estonia was devastated by the cyber attack campaign. According to *The Economist*, in 2007 Estonia was ranked 28 of 70 nations for its electronic readiness, or e-readiness.[127] Estonia also maintains an international reputation for its advanced e-governance capability. The country's investments in research and development (R&D) have yielded innovations in information and communications technology (ICT), enabling Estonia to develop the popular interface Skype and to be the first country to extend e-voting to its citizens located all over the world.[128] At the time of the cyber attacks, nearly 60 percent of Estonians conducted vital transactions online, including 95 percent of all banking transactions—making this Baltic nation an extremely attractive and lucrative target.[129] Due to the population's extensive reliance on digital communications and the absence of cybersecurity protocols, the vulnerability of Estonia was easily exploited by hackers.[130] After the

123 Buckland, Schreier, and Winkler, "Democratic Governance Challenges of Cybersecurity," 26.

124 Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, accessed May 16, 2016, http://www.iar-gwu.org/node/65, 1.

125 Richards, "Denial-of-Service," 3–4.

126 Richards, "Denial-of-Service," 4–5.

127 "E-readiness Rankings 2008: Maintaining Momentum," The Economist Intelligence Unit, 2007, http://graphics.eiu.com/upload/ibm_ereadiness_2008.pdf, 5.

128 Richards, "Denial-of-Service," 4.

129 Buckland, Schreier, and Winkler, "Democratic Governance Challenges of Cybersecurity," 26; Richards, "Denial-of-Service," 3.

130 Richards, "Denial-of-Service," 4.

Estonian government identified the botnet threat, it was able to digitally isolate its servers by blocking all international traffic.[131] The cyberwar campaign ended on May 19, 2007.[132]

While the cyber attacks against Estonia have not yet been conclusively attributed to the Kremlin, they bore the signs of Russian orchestration.[133] In fact, not only were most Estonian websites defaced with Russian nationalist propaganda, but the cyber attack tools employed by the perpetrators were also transcribed in Russian; moreover, the Russian government applauded the cyber attacks and even refused to conduct any criminal investigation.[134] According to experts from the American cybersecurity analysis firm, Delta Risk Consulting, "All signs pointed to Russian involvement."[135]

a. NATO's Immediate Response to the Estonian Cyber Attacks

Throughout the DDoS attacks against its Baltic Ally, NATO responded decisively, deploying its Computer Emergency Response Team (CERT) and employing Western intelligence to help counteract the attacks.[136] While NATO experts were unable to definitively attribute the cyber attacks to the Kremlin, the Alliance strongly condemned the aggression and privately acknowledged suspicions about Russia's role.[137]

B. CYBER ATTACKS AGAINST NATO PARTNERS

Following the DDoS attacks against a NATO Ally, Russia launched two additional cyber attack campaigns in the Alliance's periphery. These attacks were directed against two of NATO's partners, Georgia and Ukraine.

---

131 Richards, "Denial-of-Service," 5.

132 Richards, "Denial-of-Service," 5.

133 Richards, "Denial-of-Service," 5; Yost, *NATO's Balancing Act*, 45.

134 Yost, *NATO's Balancing Act*, 69.

135 Yost, *NATO's Balancing Act*, 45.

136 Herzog, "Revisiting the Estonian Cyber Attacks," 54.

137 Herzog, "Revisiting the Estonian Cyber Attacks," 53.

1. Georgia

From August 7–16, 2008, war between Russia and Georgia ensued over a geopolitical dispute regarding the Georgian territories of South Ossetia and Abkhazia, which had pro-Russian, separatist governments.[138] Russia's provocative activity in the area incited the Georgian government to mount an attack in South Ossetia, which officially started the armed conflict.[139] Russia responded with a combined military attack on Georgia, which included bombing raids, a naval blockade, a robust ground combat operation, and a coordinated cyberwarfare campaign.[140]

Russian cyber militias led DDoS strikes—similar to those orchestrated against Estonia—to disrupt Georgian communications; the cyber attacks defaced government websites with Russian propaganda and extracted military and political intelligence from Georgian servers.[141] Interestingly enough, pro-Georgian hackers responded to Russian "hacktivist" militias with their own cybernetic counter-offensives.[142] Despite these counter-attacks, the Russian military continued to demonstrate command over the cyber realm. In total, 54 Georgian websites within the government, banking, and communications sectors were attacked during the conflict.[143]

The Georgia-Russia conflict marked the first time cyberwarfare had been incorporated and synchronized with a major combat operation.[144] Yet Russia did not wait for physical warfighting to begin before it attacked in cyberspace. According to researchers, Russia began its clandestine war three weeks before bullets had even started flying.[145] Investigators discovered countless Russian-speaking chat rooms and networks

---

[138] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, (2011), http://webcache.googleusercontent.com/search?q=cache:s3_Eq_P0o4AJ:smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf+&cd=1&hl=en&ct=clnk&gl=us, 1.

[139] Hollis, "Cyberwar Case Study: Georgia 2008," 1–2.

[140] Hollis, "Cyberwar Case Study: Georgia 2008," 1–2.

[141] Hollis, "Cyberwar Case Study: Georgia 2008," 3.

[142] Hollis, "Cyberwar Case Study: Georgia 2008," 3.

[143] Hollis, "Cyberwar Case Study: Georgia 2008," 2.

[144] Hollis, "Cyberwar Case Study: Georgia 2008," 2.

[145] Hollis, "Cyberwar Case Study: Georgia 2008," 2.

that had discussed the upcoming cyber attacks for weeks.[146] Indeed, Russia's armed forces regularly targeted Georgian sites physically only after they had first targeted them cybernetically.[147]

a. NATO's Immediate Response to the Georgian Cyber Attacks

The Georgia-Russia war occurred just four months after the Alliance had postponed any decision on offering Georgia and Ukraine Membership Action Plan (MAP) status at the 2008 Bucharest Summit.[148] Owing in part to the fact that Georgia was a NATO partner and active in NATO-led crisis management operations, the Alliance strongly condemned Russia's actions in Abkhazia and South Ossetia.[149] Additionally, NATO called for a ceasefire a day after hostilities erupted.[150] While Russia's cyberwarfare campaign against Georgia shut down numerous websites, the digital attacks were overall less disruptive in Georgia than they were in Estonia, since Georgia's economic and political infrastructure had a much smaller online presence.[151] The conflict ended approximately 10 days after the initial skirmish in South Ossetia.[152]

2. Ukraine

In February 2014, much of the world was caught off guard when Russian troops invaded Crimea. What began as a political dispute between Russia and Ukraine over a failed trade deal with the European Union (EU) ended with domestic unrest, an ousted president (Viktor Yanukovich), and a strategic opportunity fully exploited by Vladimir Putin. Within just a few weeks, Russia held a local referendum, successfully annexed the

146 Hollis, "Cyberwar Case Study: Georgia 2008," 4.

147 Hollis, "Cyberwar Case Study: Georgia 2008," 5.

148 Adam Taylor, "That Time Ukraine Tried to Join NATO—and NATO Said No," *Washington Post*, September 4, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/09/04/that-time-ukraine-tried-to-join-nato-and-nato-said-no/, 2.

149 "2008 Georgia Russia Conflict Fast Facts," CNN, March 21, 2016, http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/, 3.

150 "2008 Georgia Russia Conflict Fast Facts," 3.

151 Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 28.

152 Hollis, "Cyberwar Case Study: Georgia 2008," 1–2.

Crimean Peninsula, and started a proxy war in the Donbas region of Ukraine, which has left over 6,000 dead and counting.[153]

While Russia accomplished the Crimean annexation through traditional military means, it started its destabilization campaign using hybrid or "modern warfare," which consisted of disinformation, psychological and deception operations, and cyber intrusions.[154] LookingGlass Cyber Solutions, a security firm based in Arlington, Virginia, released a report in 2015 confirming that since 2013, Russia had embarked on a coordinated cyber espionage campaign—termed Operation Armageddon—which targeted the Ukrainian government, law enforcement, and military.[155] Using simple spear phishing tactics,[156] Russian cyber attackers were able to conceal malware in the attachments of official-looking electronic correspondence; once opened, the attachments infected Ukrainian networks and extracted intelligence that was highly valuable to the Russian war effort.[157] Much of the classified and sensitive intelligence collected by hackers included information on Ukrainian military equipment, battalion troop numbers, and combat action plans, including the positions of Ukrainian forces, targets, and more.[158] Consequently, the Ukrainian government lost many strategic advantages to Russia due to cyber vulnerabilities. As with Russia's strategy during the Georgia-Russia war, Russian hackers

153 "Ukraine Crisis: Timeline of Major Events," *The Telegraph,* March 5, 2015, http://www.telegraph.co.uk/news/worldnews/europe/ukraine/11449122/Ukraine-crisis-timeline-of-major-events.html, 2–3.

154 Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War,'" *Kennan Cable*, no. 7 (2015): 1–8, https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf, 2–3.

155 "LookingGlass Cyber Threat Intelligence Group Links Russia to Cyber Espionage Campaign Targeting Ukrainian Government and Military Officials," LookingGlass, April 29, 2015, https://lgscout.com/press-release/lookingglass-cyber-threat-intelligence-group-links-russia-to-cyber-espionage-campaign-targeting-ukrainian-government-and-military-officials/, 1.

156 Spear phishing tactics are cyber methods used to steal information; some spear phishing methods employ malware, spyware, and spam. (Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 14).

157 "LookingGlass Cyber Threat Intelligence Group," 1–2.

158 Aarti Shahani, "Report: To Aid Combat, Russia Wages Cyberwar against Ukraine," April 28, 2015, http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine, 2.

used unsophisticated yet effective cyberwarfare and espionage tactics in synchronization with kinetic military attacks.[159]

Russia's cyber operations in Ukraine have been a blend of the methods and techniques observed in the Estonian and Georgian cases. The Kremlin's cybernetic activities in Ukraine have focused on intelligence collection to enhance the effectiveness of its ground campaign—a strategy nearly identical to Moscow's actions in the Georgian conflict; however, Russian activities in Ukraine have also involved access denial attacks comparable to those observed in both Georgia and Estonia.[160] The Kremlin employed DDoS attacks on Ukrainian political and media sites, defaced various NATO sites with Russian propaganda, leaked classified Ukrainian government information, and disrupted Ukrainian telecommunications and networks..[161] As for attribution, many of the Allies suspected that Russian state-sponsored hackers and volunteer cyber militias perpetrated the cyber attacks against Estonia.[162] In Ukraine, moreover, the Allies widely regard Russia's state security service—the FSB—as the culprit, although evidence has been circumstantial.[163]

a. NATO's Immediate Response to the Ukrainian Cyber Attacks

In the wake of Russia's hybrid attacks during the Ukraine crisis, NATO denounced Russia's illegitimate actions, calling for Moscow to terminate its military occupation and end its destabilization efforts in the region.[164] Immediately after the Wales Summit in 2014, NATO leaders reaffirmed support for Ukraine's sovereignty, establishing five security trust funds to help Ukraine improve its defense capabilities; one of those funds was

159 "LookingGlass Cyber Threat Intelligence Group," 1.

160 Jarno Limnell, "Putin is Waging a Relentless Cyberwar Against Ukraine," *Newsweek*, January 11, 2016, http://www.newsweek.com/putin-cyberwar-ukraine-russia-414040, 2.

161 Limnell, "Putin is Waging a Relentless Cyberwar Against Ukraine," 2.

162 Yost, *NATO's Balancing Act*, 45, 69.

163 Shahani, "Report: To Aid Combat, Russia Wages Cyberwar against Ukraine," 3.

164 "NATO Stands Firm in Support for Ukraine," NATO, May 13, 2015, http://www.nato.int/cps/en/natohq/news_119420.htm, 1–2.

for cyber defense.[165] Under the Cyber Defense Trust Fund, NATO Allies have provided technical training, equipment, and assistance to Ukraine to help establish an Incident Management Center for monitoring and responding to incidents in cyberspace.[166] At the 2016 Warsaw Summit, the Alliance reiterated the commitment to its partnership with Ukraine by issuing the following statement: "We stand firm in our support for Ukraine's sovereignty and territorial integrity within its internationally recognized borders and Ukraine's right to decide its own future and foreign policy course free from outside interference, as set out in the Helsinki Final Act."[167]

165 "NATO's Practical Support to Ukraine," NATO, December 2015, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf, 1.

166 "NATO's Practical Support to Ukraine," 1.

167 "Warsaw Summit Communiqué," par. 117.

V. NATO'S LEVEL OF PREPAREDNESS

This thesis performs a qualitative analysis of NATO's preparedness for cyberwar by evaluating the Alliance's cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization. How successfully NATO performs across these seven areas will indicate its probable level of preparedness for combating a major terrorist or state-sponsored cyber attack effectively.

A. CYBER STRATEGY

In the wake of the cyber attacks against Estonia and Georgia, NATO made significant policy and organizational changes, some of which were already under development before these attacks. One year after the 2007 attacks against Estonia, NATO opened its cyber policy and research center, the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia.[168] In January 2008, NATO also released its first strategy on cybersecurity, the Cyber Defense Policy, which was formally endorsed at the Bucharest Summit.[169] At the 2014 Wales Summit, NATO heads of state and government formally endorsed a new cyber strategy—the Enhanced NATO Policy on Cyber Defense—which affirmed NATO's commitment to information-sharing, cooperation with industry and international organizations, and to the defense of Alliance networks.[170] NATO made additional progress toward cybersecurity at the 2016 Warsaw Summit, at which the Alliance formally recognized cyberspace as comparable in strategic importance to the three conventional warfighting domains—air, land, and sea.[171] In an effort to assess the Alliance's readiness for cyberwar, the thesis evaluates the quality of NATO's cyber strategy across three areas: comprehensiveness, execution, and clarity.

168 Richards, "Denial-of-Service," 6.

169 Healey and Jordan, "NATO's Cyber Capabilities," 2.

170 "NATO Summit Updates Cyber Defense Policy," CCDCOE, October 24, 2014, https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html#footnote3_buq6aol, 1.

171 "Warsaw Summit Communiqué," par. 70.

1. Comprehensiveness

Over the years, NATO has taken significant steps to improve the depth and breadth of its cybersecurity strategy in order to address the evolving and persistent nature of cybernetic threats and attacks. In 2011, NATO revised its cyber defense strategy—an action which underscored the importance for the Alliance to strengthen its cyber capabilities in detection, defense, and response.[172] By 2014, NATO released the Enhanced NATO Policy on Cyber Defense, a classified document.[173]

The Enhanced NATO Policy on Cyber Defense provides specific guidance on improving network capabilities and system set-up for cyber defense, detection, resilience, redundancy, and recovery.[174] The policy outlines multiple ways to safeguard the Alliance's information systems; in fact, it provides guidance on intrusion-prevention, network resiliency, and response capability.[175] For the first time, NATO set minimum security requirements for Allied networks and incorporated cybersecurity requirements into the NATO Defense Planning Process (NDPP).[176] With the adoption of a unified policy on cyber defense, NATO also created the Cyber Defense Management Authority (CDMA) to integrate and consolidate its digital defense capabilities.[177]

One way in which NATO protects its digital data and adheres to the cybersecurity protocols recommended by its cyber strategy is by storing its most sensitive information on remote locations inaccessible from the Internet.[178] Another way in which NATO prepares its cybernetic defenses is by assuming its systems have already been breached, thereby improving network awareness while bridging vulnerability gaps and avoiding complacency.[179] Vigilance and planning are critical aspects of the Alliance's

172 "Defending the Networks," 1.

173 "Men in Black," 1.

174 "Men in Black," 1.

175 Healey and Jordan, "NATO's Cyber Capabilities," 2, 6.

176 "Defending the Networks," 1.

177 Herzog, "Revisiting the Estonian Cyber Attacks," 54.

178 Tony Morbin, "NATO: Defending Against the Known Unknowns," *SC Magazine UK*, 2015, http://www.scmagazineuk.com/nato-defending-agains-the-known-unknowns/article/400190/, 1.

179 Morbin, "NATO: Defending Against the Known Unknowns," 1.

comprehensive strategic approach toward cybersecurity. In fact, NATO has taken great strides in integrating its cybersecurity strategy into its operational and crisis response planning processes.[180] In September 2015, NATO's defense ministers endorsed a new Military Concept for Cyber Defense to improve cybersecurity planning within the Alliance's military structure.[181]

NATO also employs its centers of excellence as resources for training, research, and strategy development. The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) published a guide in 2012 on cybersecurity called the *National Cybersecurity Framework Manual*.[182] The document provides specific guidance to state actors on integrating cybersecurity into their national strategies, engaging private and public industry effectively, and incorporating diversified defensive cyber approaches into network solutions.[183] While this framework offers a comprehensive national approach to cyber, it is only a recommendation for adoption because NATO does not fund the CCDCOE nor endorse the publications it releases.[184] By convention, the Alliance cannot mandate adherence to the principles of the CCDCOE's national guide, and this represents an organizational shortfall. Nevertheless, the Alliance has taken tangible steps to integrate cyber defense into its policies, planning, missions, command structure, and decision-making processes.[185] By 2012, the Alliance began implementing many of the defense requirements of its cybersecurity policy.[186]

---

180 Jens Stoltenberg, *The Secretary General's Annual Report 2015*, NATO, 2015, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160128_SG_AnnualReport_2015_en.pdf, 23.

181 Stoltenberg, *Secretary General's Annual Report 2015*, 23.

182 Alexander Klimburg, ed., *National Cybersecurity Framework Manual* (Tallinn: NATO CCD COE, 2012), https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

183 Klimburg, *National Cybersecurity Framework Manual*, v-viii.

184 Klimburg, *National Cybersecurity Framework Manual*, iv.

185 "Cybersecurity," NATO, last modified July 9, 2015, http://www.nato.int/cps/en/natohq/topics_78170.htm, 5.

186 "Cybersecurity," 5.

2. Execution

NATO's execution of its cyber strategy is reflected in its revised command structure, which is now comprised of key cyber agencies and organizations, including the NATO Cyber Incident Response Capability (NCIRC) Center, the Communications and Information Systems (CIS) Group, and NATO's Rapid Reaction Teams (RRTs). The NCIRC—established in 2012—acts as the Alliance's cyber center of gravity, providing 24/7 information technology (IT) management and cyber defense support to 41 NATO sites located in Europe and North America.[187] As NATO's main staff element, it liaises with international stakeholders like the European Union (EU), the United Nations (UN) International Telecommunication Union (ITU), and the Organization for Security and Cooperation in Europe (OSCE) on cybersecurity matters.[188] The NCIRC also serves as the central coordination agency for preventative and responsive cyber solutions for the Alliance's networks.[189] In the event of a major cyber attack, the NCIRC activates a rapid NATO-wide response for system repair and recovery.[190] On certain occasions, the Rapid Reaction Teams (RRTs) are called to respond.[191] NATO's RRTs are relatively small units of cybersecurity experts (typically four to six people), who can offer on-site technical support to Allies and NATO sites that have suffered significant cyber-attacks.[192] The NATO CIS Group in Mons, Belgium—also established in 2012—provides deployable IT experts located across the European theater to Allied nations for operational support, technical assistance, and exercises.[193]

---

187 Anil Suleyman, "NCIRC (NATO Computer Incident Response Capability)," 11th TF-CSIRT Meeting, Madrid, Spain January 15, 2004, https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf, 4–5, 10; Stoltenberg, *Secretary General's Annual Report 2015*, 23.

188 "Cybersecurity," 4.

189 Suleyman, "NCIRC," 1.

190 Suleyman, "NCIRC," 4–5.

191 "Men in Black," 2.

192 "Men in Black," 1.

193 "Allied Command Operations (ACO)," NATO, last modified November 11, 2014, http://www.nato.int/cps/en/natolive/topics_52091.htm, 3; NATO, "NATO CIS Group Adds New Unit in Croatia," April 7, 2014, http://www.aco.nato.int/nato-cis-group-adds-new-unit-in-croatia.aspx, 1.

As part of its command reform in 2012, the Alliance also established NATO's Communications and Information Organization (NCIO), which performs command, control, communications, information, and cyber defense functions for the Allies.[194] Part of NATO's Smart Defense and Connected Forces initiatives, the NCIO is one of the Alliance's largest organizations.[195] The NCIO is made up of two entities: an Agency Supervisory Board comprised of 28 representatives (one from each Allied nation) and the NATO Communications and Information Agency (NCIA), an organization that serves as the NCIO's main executive body, staffed by 200 people.[196] The NCIA—the organization's main consultation, command, and control entity—offers another layer of IT support for NATO's headquarters and external agencies.[197] Like the Cyber Defense Management Authority (CMDA), the NCIA is responsible for identifying operational requirements and carrying out the Alliance's cybernetic defense activities.[198] The NCIA's daily activities range from monitoring hundreds of cyber intrusion sensors, email servers, and NATO websites to conducting network vulnerability testing and cybersecurity training.[199] Through these cyber agencies and resources, NATO can manage and resolve millions of cyber intrusions before they rise to the level of a major breach.[200]

Although NATO's cyber policies have assisted Allied nations in strengthening their network defenses and cybernetic capabilities,[201] NATO as a whole safeguards, manages, and asserts responsibility for its own internal networks; it has historically

194 "NATO Communications and Information Agency (NCI Agency)," NATO, April 7, 2016, http://www.nato.int/cps/en/natolive/topics_69332.htm, 1–2; "NATO Internship Program: NATO Communications and Information Organization (NCIO)," NATO, March 11, 2011, http://www.nato.int/cps/en/natolive/71161.htm, 1.

195 "NATO Internship Program: NATO Communications and Information Organization (NCIO)," 1.

196 "NATO Internship Program: NATO Communications and Information Organization (NCIO)," 1; "NATO Communications and Information Agency," 1; Morbin, "NATO: Defending Against the Known Unknowns," 1.

197 "Cybersecurity," 5; "NATO Communications and Information Agency," 1.

198 "Cybersecurity," 3.

199 Morbin, "NATO: Defending Against the Known Unknowns," 1.

200 "Men in Black," 1–3.

201 "Men in Black," 1.

accepted minimal responsibility for maintaining day-to-day cybersecurity for its individual members.[202] By convention, NATO encourages its Allies to assume responsibility for the defense of national networks.[203] Multiple Alliance members, including France, Germany, the UK, and the United States, also regard cybersecurity as a national responsibility.[204] Nonetheless, in the spirit of solidarity and according to NATO analysts (from the Author's conversations in Brussels, Belgium, September 15–17, 2015), NATO's policy is to offer technical support and training to Allies who request assistance.

If an Ally experiences a cyber crisis, it can petition the North Atlantic Council (NAC), the main political decision-making body of the Alliance, to deploy a Rapid Reaction Team (RRT) or a unit from the NATO Communications and Information Systems (CIS) Group for support.[205] If the problem is large enough, as in the 2007 Estonia case, NATO can also deploy national Computer Emergency Response Teams (CERTs) to resolve the incident and restore the affected Ally's systems.[206] In this way, NATO would not have to wait for an Article 5 invocation to respond to cyber aggression against one or more of its members; it could employ responsive measures preceding or following an official call for collective defense.

3. Clarity

NATO's publicly declared policy on cyber threats is consciously and purposefully vague.[207] Why? Strategic ambiguity has its benefits. According to the Atlantic Council panel, there is no "redline" or "determined threshold" that would automatically define a cyber act as an act of war.[208] Leaving the rules undefined affords NATO ample room in which to operate. For a 28-member multinational organization that operates on the

202 Yost, *NATO's Balancing Act*, 47.

203 "Wales Summit Declaration," par. 72.

204 Yost, *NATO's Balancing Act*, 47.

205 "Men in Black," 2.

206 Herzog, "Revisiting the Estonian Cyber Attacks," 54.

207 Sydney J. Freedberg, Jr., "NATO Hews to Strategic Ambiguity on Cyber Deterrence," *Breaking Defense*, November 7, 2014, http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/, 2.

208 Freedberg, "NATO Hews to Strategic Ambiguity," 1.

principle of consensus, time and latitude for solidifying strategic-level decisions are critical. If NATO publicized a cyber redline, it would box the Alliance into a corner. This kind of policy could embolden cyber offenders and provoke massive intrusions that target NATO's networks at just below this threshold. Having a defined redline could also invite nefarious cyber actors to cross it to test NATO's resolve, damage its reputation as a leader in Euro-Atlantic security, and undermine the credibility of its Article 5 commitments.

Following the Wales Summit in 2014, NATO affirmed its stance on law and cyberspace while refusing to address cyber redlines:

> Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm, therefore, that cyber defense is part of NATO's core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.[209]

However, an invocation of Article 5 does not necessarily mean that a NATO response would include force. Article 5 of the Washington Treaty states the following:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[210]

Thus, as long as each Alliance member takes "such action as it deems necessary," it cannot be found in violation of the collective defense principle.[211] In the case of a

209 "Wales Summit Declaration," par. 72.

210 "The North Atlantic Treaty," NATO, April 4, 1949, Washington, D.C., http://www.nato.int/cps/en/natolive/official_texts_17120.htm, Article 5.

211 "North Atlantic Treaty," Article 5.

major act of cyberwar against one of its members, NATO could invoke Article 5 as a show of solidarity but opt to refrain from employing kinetic military force; instead, the Alliance could use purely cybernetic means or a hybrid alternative that combined cybernetic tools with military force to fulfill its objectives.

In all, NATO's establishment, organization, and employment of its sophisticated cyber response agencies and IT resources like the NCIRC, NCIO, NCIA, and RRT are indicative of how seriously the Alliance has implemented its cyber defense policies at the operational level. NATO's cyber policy, standard operating procedures, and ambiguous thresholds for the use of military force make the Alliance highly prepared to respond effectively to major acts of cyber aggression against one or more of its members. If an act of cyberwar met the threshold of an armed attack, NATO would probably be prepared to manage, counter, and resolve the issue in cyberspace; still, one cannot exclude the possible need to take kinetic measures. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 3 in cyber strategy.

B. CYBER COOPERATION

The Alliance understands that being prepared for cyber attacks does not mean only being ready to respond with an Article 5 invocation. To NATO, it also means being able to respond digitally with innovative resources and tools to minimize damage to its own and to every member-state's network infrastructure. One way NATO improves its technical capability is through cyber partnerships solidified through cooperation.

1. Exercises

NATO leads several annual cyber-related exercises with its members, including Locked Shields, which is a real-time network defense event that employs realistic attack models in a game-based setting.[212] In 2015, Locked Shields brought together approximately 400 participants from 16 countries to practice the latest cyber defense solutions.[213] NATO also leads exercise Steadfast Cobalt, which tests command, control,

[212] "Cyber Security Training Events," CCDCOE, accessed August 27, 2015, https://ccdcoe.org/events.html, 1.

[213] Stoltenberg, *Secretary General's Annual Report 2015*, 23.

communications, computers, and information (C4I) management capability, including interoperability and connectivity among the NATO Reaction Force (NRF), the Very High Readiness Joint Task Force (VHRJTF), and national communications and information systems (CIS) units.[214] In 2015, NATO conducted its Cyber Coalition exercise in Estonia with nearly 750 participants from over 33 nations.[215] The Alliance also incorporates cyber defense into other joint and tactical exercises, including Trident Jaguar, Trident Jewel, Baltic Ghost, and its largest exercise—Trident Juncture.[216]

2. Education and Training

NATO operates a Communications and Information Systems (CIS) School in Latina, Italy that offers 124 courses on information technology (IT) management, operations, and maintenance.[217] The advanced IT and cyber defense courses provide cost-effective training solutions to NATO command personnel, Alliance members, and Partnership for Peace nations.[218] The Cooperative Cyber Defense Center of Excellence (CCDCOE) in Estonia also offers free technical courses to Alliance members on botnet, malware, and digital forensic training.[219] Both the NCISS and the CCDCOE offer mobile training teams to deliver on site instruction on various cyber-related topics.

3. Workshops and Conferences

The Alliance, in cooperation with the CCDCOE, hosts numerous workshops annually. Many of these events, including Countering Botnets, Cyber Norms and International Relations, Ethics of Cyber Conflict, Human Rights in Cyberspace, and the Joint Monitoring and Forensics workshops, help disseminate the latest information on

---

214 "Exercise Steadfast Cobalt Tests NATO's Communications Systems," NATO, June 4, 2015, http://www.aco.nato.int/exercise-steadfast-cobalt-tests-natos-communications-systems-2.aspx, 1–2.

215 Stoltenberg, *Secretary General's Annual Report 2015*, 23.

216 "NATO CCDCOE Command Brief," NATO Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, January 8, 2015.

217 "NATO Communications and Information Systems School: Courses—Course Descriptions," NATO, accessed August 27, 2015, http://www.nciss.nato.int/courses_description.php, 1–2.

218 "NATO Communications and Information Systems School: About Us—Mission," NATO, accessed August 27, 2015, http://www.nciss.nato.int/mission.php, 1."

219 "Cyber Security Training Events," 1.

evolving norms, defense tools, and legal policies in the cyber domain.[220] Additionally, NATO leads the annual Cybersecurity Conference, which brings together multinational private and government industry experts to discuss cyber trends and share innovations in cyber-based solutions.[221]

4. Initiatives

NATO sponsors programs and initiatives that have broadened its partnerships with private industry and partner nations on cyber-related issues. For example, NATO's Science for Peace and Security (SPS) program supports initiatives with the public sector and multinational governments to streamline cooperation on information technology (IT) techniques, research and development (R&D), incident response, and information-sharing.[222] As of 2015, the SPS had nine cyber defense projects either ongoing, under development, or scheduled.[223] In addition, NATO works closely with the Organization for Security Cooperation in Europe (OSCE) to promote security-building measures and enhance information cooperation in cyberspace.[224] Moreover, as part of the Smart Defense project, 20 Allies and two partner nations contribute to NATO's cybersecurity initiatives.[225] In 2015, the Allies signed the Cyber Defense Memorandum of Understanding, designed to improve information sharing among NATO and national cyber defense agencies and authorities.[226] The Alliance also leads cyber initiatives with non-NATO partners. For example, NATO collaborates with partners in the South Caucasus region on cybernetic matters to build trust, promote dialogue on shared issues, and develop defensive adaptive approaches.[227] The Alliance regards its political outreach and cooperative cyber initiatives as effective instruments for strategic success. With such

220 "Cyber Security Training Events."

221 "Cyber Security Training Events."

222 "Enhanced Cyber Defense Cooperation in the South Caucasus and Black Sea Region," NATO, July 29, 2015, http://www.nato.int/cps/en/natohq/news_121969.htm, 2.

223 Stoltenberg, *Secretary General's Annual Report 2015*, 23.

224 Stoltenberg, *Secretary General's Annual Report 2015*, 23

225 Stoltenberg, *Secretary General's Annual Report 2015*, 23.

226 Stoltenberg, *Secretary General's Annual Report 2015*, 23.

227 "Enhanced Cyber Defense Cooperation," 3.

a progressive and inclusive outlook, NATO is moving in a positive direction toward cyber preparedness.

While information-sharing makes up a critical part of NATO's cyber readiness, it also represents a major hurdle for the Allies. Information-sharing in the cyber domain tends to be greater among corporations than among governments. In fact, cyber heavyweights like the Governments of the UK and the United States are reluctant to share classified cyber intelligence among their Allies because information assurance and protection are weak within some member states (as conveyed by NATO analysts in Brussels, Belgium, September 15–17, 2015). Nevertheless, as Allies invest more in their critical cybernetic infrastructures and improve the security of their systems, NATO may well increase the level of intra-Alliance information-sharing.

Today, NATO's overall level of cyber cooperation makes it highly prepared to effectively address and counter major acts of cyber aggression against one or more of the Allies. If an act of cyberwar met the threshold of an armed attack, the Allies today would probably be adequately prepared to call upon one another for assistance. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 3 in cyber cooperation.

C. DECISION MAKING

NATO maintains an integrated command structure comprised of a permanent civilian element, the North Atlantic Council (NAC), and a permanent military component, the Military Committee (MC).[228] The NAC is the top decision-making body of the Alliance, and it sometimes operates using a "silence procedure" to obtain consensus among the 28 member states.[229] In such cases, when a decision is put to a vote, silence means consent; when nations oppose a policy decision, they can "break silence" by writing a letter to the Secretary General within a specified timeframe explaining their

[228] Paul Gallis, *NATO's Decision-making Procedure* (CRS Report No. RS21510), Washington, DC: Congressional Research Service, 2003, fas.org/man/crs/RS21510.pdf, 2.

[229] Michel, "NATO Decision Making," 1; Gallis, "NATO's Decision-making Procedure," 3.

objections.[230] This decision-making protocol reflects the equality and value of each member.[231] The discretion of the consensus rule enables Alliance members to avoid confrontation on policy objections.[232] Since an Ally's acquiescence to a collective decision does not obligate it to actively support the proposed policy, the passive nature of the consensus rule allows member states to meet their Alliance commitments while avoiding politically contentious issues on the domestic front.[233]

Although opponents of the consensus rule assert that NATO should streamline its decision-making process, there is some evidence to suggest the consensus rule has not significantly slowed down or reduced the effectiveness of NATO's decision-making capability. For example, it took only 24 hours for the Alliance to make the unprecedented decision to invoke Article 5 following the September terrorist attacks.[234] In this case, a lack of precedent did not prevent the Alliance from acting quickly and decisively. Nonetheless, in the realm of cyber in which millions of attacks may happen within nanoseconds, cyber or hybrid contingencies that include a cyber dimension require quicker decision making.

Indeed, hybrid warfare significantly alters the strategic playing field, giving home field advantage to the perpetrators while muddying the view for the target and observers. This ambiguity slows down normal decision making for state actors and organizations, especially NATO. In fact, during Russia's Crimea annexation, some NATO strategists contended that the Alliance took too long to respond.[235] Many of NATO's senior leaders, including General Denis Mercier, the Supreme Allied Commander for Transformation,

230 Gallis, "NATO's Decision-making Procedure," 3.

231 Gallis, "NATO's Decision-making Procedure," 3.

232 Gallis, "NATO's Decision-making Procedure," 3.

233 Michel, "NATO Decision Making," 2–3.

234 Michel, "NATO Decision Making," 3.

235 Sam Jones, "NATO Top Brass Urges Political Leaders to be as Ready as Soldiers," *Financial Times,* August 7, 2016, http://www.ft.com/cms/s/0/0455dcb2-55a7-11e6-9664-e0bdc13c3bef.html#axzz4HVXxHOKq, 2.

believe that NATO's political decision making and intelligence analysis processes need to be accelerated for the Alliance to uphold its security guarantees to its members.[236]

In the case of a terrorist or state-sponsored cyber attack that threatens Allied security, the decision to invoke Article 5 would first go to the NAC. Depending on various factors such as the type of cyber attack, the level of destruction, the timeliness and certainty of attribution, and the Alliance's strategic messaging goals, NATO might invoke Article 5. Still, this invocation would not obligate the Alliance to respond against the aggressor nation with military force. The NAC would decide on an appropriate response, which might not include military measures. The menu of options that NATO could exercise might realistically include a blend of defensive cyber measures to increase deterrence and enhance the resiliency of the affected Ally's network infrastructure.

Still, before NATO invokes Article 5, it has other options at its disposal. NATO has a sophisticated cyber capability—including experts on cybersecurity, intrusion detection, and computer forensics—that it could activate following a NAC decision to combat a cyber act of aggression.[237] As this thesis has previously discussed, NATO's Rapid Reaction Teams (RRTs) can deploy on short notice upon a request to offer technical assistance to NATO facilities and Allied members that suffer network intrusions.[238] Each day, the NCIRC Center analyzes and responds to over 200 million cyber incidents that take place on NATO's networks—ten of which on average are sophisticated attacks requiring action by the RRT.[239] According to NATO experts (expressed during the author's conversations in Brussels, Belgium, September 17, 2015), although the NAC deploys the RRT daily for its own network security, it has yet to do so on behalf of an Ally. Because a decision to deploy the RRT must be reached by the NAC, protocol might impede the team's future efficacy in cyber response, at least in some circumstances. Thus, NATO's ability to act quickly on behalf of an Ally attacked in cyberspace could be impeded by its bureaucratic consensus model.

---

236 Jones, "NATO Top Brass Urges Political Leaders to be as Ready as Soldiers," 2–3.

237 "Men in Black," 2.

238 "Men in Black," 1.

239 "Men in Black," 2.

The RRT offers the Alliance increased options in its decision-making matrix at the operational level of cyber warfare. With the continuing transformation and evolution of NATO, the organization is finding more ways to increase its flexibility, options for intervention, response capability, and overall preparedness.[240] Nevertheless, the Alliance must seek new ways to ensure that its response is not delayed by its political processes. By delegating a greater degree of autonomy to its cyber teams, including the Computer Emergency Response Team (CERT) and Rapid Reaction Team (RRT), NATO would be better prepared to respond to an act of cyberwar against one or more of the Allies. The Alliance's current decision-making processes and protocols are moderately prepared to respond cybernetically to major acts of cyberwar. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 2 in decision making.

D. POLITICAL WILL

In any situation regarding a potential employment of force, the geostrategic and domestic political situation of each member state will factor heavily into NATO's decision-making calculus. In September 2008, a poll published by the *Financial Times* revealed that the publics in three NATO member states—Germany, Italy, and Spain—would not support the employment of their national armed forces to defend Estonia, Latvia, and Lithuania if these nations were attacked.[241] In contrast, a majority of the publics in France and the UK supported honoring their Article 5 commitments to defend their Baltic Allies.[242] Some NATO Allies, including the Baltic states, the Czech Republic, and Poland, have long voiced concerns regarding the political will of fellow Alliance members to honor their collective defense commitments.[243] Indeed, in the wake of Russian aggression in Georgia and Ukraine, many of the Central and Eastern European Allies have expressed anxiety about the political and military resolve of the Alliance to respond to a Russian hybrid war campaign launched against a NATO member.[244]

---

240 "Men in Black," 2; "Allied Command Operations (ACO)," 3.

241 Yost, *NATO's Balancing Act*, 35.

242 Yost, *NATO's Balancing Act*, 35.

243 Yost, *NATO's Balancing Act*, 35.

244 Yost, *NATO's Balancing Act*, 35.

A study undertaken by the Pew Research Center in the spring of 2015, which surveyed public opinion across eight NATO countries—Canada, France, Germany, Italy, Poland, Spain, the UK, and the United States—also showed a large divide in the willingness of these populaces to use military force to defend a NATO Ally attacked by Russia.[245] While the willingness of support across the Allied nations surveyed averaged only around 47 percent, the countries that most clearly supported a use of force to defend a NATO Ally were Canada and the United States at 53 percent and 56 percent, respectively.[246] The two nations least favorable to responding with force were Germany and Italy at 38 percent and 40 percent, respectively.[247] Additionally, the study showed that American public support for Article 5 is down from 82 percent in 1956 to 56 percent in 2015.[248] This finding may indicate that America's war-weariness has affected its willingness to come to the aid of an Ally in need. German support for NATO in general is down slightly from 59 percent in 2013 to 55 percent in 2015.[249] These views, coupled with Germany's growing diplomatic power in Europe, may have a negative impact on NATO's decision making and cohesion.[250] Although a 2016 Pew study showed that many Allied publics held favorable views of NATO (a median of 57 percent surveyed across 11 member states), the question of collective defense was never examined.[251] In all, the 2008 and 2015 Pew research findings suggest that support for any NATO-led military campaign—in the name of collective defense—is in marked decline.

Additional factors complicating the political will of the Alliance include nationalism. The sweeping rise of nationalist parties across Europe could produce devastating consequences for Euro-Atlantic security. Indeed, the EU is currently bearing

---

245 Naftali Bendavid, "Opinion in NATO Countries Varies Widely on Russia, Ukraine," *The Wall Street Journal*, June 10, 2015, http://www.wsj.com/articles/opinion-in-nato-countries-varies-widely-on-russia-ukraine-1433909106, 1.

246 Bendavid, "Opinion in NATO Countries Varies Widely," 1.

247 Bendavid, "Opinion in NATO Countries Varies Widely," 1.

248 Bendavid, "Opinion in NATO Countries Varies Widely," 2.

249 Bendavid, "Opinion in NATO Countries Varies Widely," 2.

250 Bendavid, "Opinion in NATO Countries Varies Widely," 3.

251 Danielle Cuddington, "Support for NATO is Widespread among Member Nations," Fact Tank, July 6, 2016, http://www.pewresearch.org/fact-tank/2016/07/06/support-for-nato-is-widespread-among-member-nations/, 1.

witness to the tumultuous effects of nationalist movements. The British public's fears of supranational institutions usurping control over the nation's political freedoms, sovereignty, and rights to self-determination are among the chief factors that drove it to vote to leave the EU. Moreover, the meteoric rise of French presidential candidate Marine Le Pen on a nationalist platform—that is, a platform in favor of a greater, more independent France—illustrates how nationalism could threaten the cohesion of the EU and NATO.[252] Le Pen, who is currently expected to advance to the second round of voting in the 2017 French presidential elections,[253] has advocated a dissolution of the EU, a return to the French Franc, and a withdrawal from NATO's integrated defense structure (which France just rejoined in 2009).[254] If France weakens its role in NATO and/or the EU, this could signify negative strategic implications for the Alliance. In fact, NATO's adversaries—especially Russia—would exploit any divisions within the Alliance, including fractures in its military and strategic solidarity.

In July 2016, U.S. Republican presidential nominee Donald Trump sent shockwaves through the Alliance by declaring that, if elected president, he would not guarantee that the United States would uphold its Article 5 commitments.[255] Trump justified his stance—which clashed fundamentally with historical U.S. policies on NATO—with the fact that 23 of 28 Allies do not currently meet NATO's 2 percent defense spending guideline.[256] According to Trump, if the Allies "aren't paying their bills" to the Alliance, they should not reap the defense benefits.[257] This is a seemingly logical argument—except that NATO's 2 percent of Gross Domestic Product (GDP) spending guideline is a recommendation, not a requirement. Nor is this spending

252 Leo Michel, "Why Americans Should Worry about Marine Le Pen," Atlantic Council, December 2015, http://www.atlanticcouncil.org/blogs/new-atlanticist/why-americans-should-worry-about-marine-le-pen, 2.

253 James Newell, "Italy's Looming Referendum is Giving PM Matteo Renzi Sleepless Nights," August 15, 2016, http://theconversation.com/italys-looming-referendum-is-giving-pm-matteo-renzi-sleepless-nights-63844, 1.

254 Michel, "Why Americans Should Worry," 2.

255 Richard Milne, "Trump's Baltic Shift Sends Shivers through Region's Capitals," *Financial Times*, August 1, 2016, 1.

256 Milne, "Trump's Baltic Shift," 2.

257 Milne, "Trump's Baltic Shift," 2.

guideline a part of the 1949 North Atlantic Treaty, since it was agreed upon in 2006.[258] For the Allies most exposed to an attack—Estonia, Latvia, Lithuania, and Poland—this declaration from the prospective head of state of their strongest and closest Ally is alarming.[259] If Trump was elected president, his statements could undermine the political progress the United States has made through its billion-dollar European Reassurance Initiative (ERI) program, begun in June 2014 in the aftermath of Russian aggression in Crimea and Ukraine.[260] Through increased U.S. military presence in Eastern and Central Europe, the initiative has attempted to reassure NATO's Allies and partners of American resolve and commitment to their security and territorial integrity.[261] Now, with Trump's imprudent remarks, the United States risks signaling to Moscow that it will not stand in its way if Russia decides to threaten its NATO neighbors.[262] Anders Fogh Rasmussen, a former NATO Secretary General, has expressed similar judgments regarding this issue.[263]

Although NATO's one-nation, one-vote consensus principle reinforces the idea that each Ally is equal, is this in fact the case in the eyes of specific Allies? The nations surveyed during the 2008 and 2015 Pew studies are among the Alliance's top security contributors. Indeed, many of them also have the largest political influence within NATO. Their reluctance to employ force to protect fellow Allies could corrode the Alliance's solidarity and adversely influence future defense policies.

---

258 "Funding NATO," NATO, June 3, 2015, http://www.nato.int/cps/en/natohq/topics_67655.htm, 1.

259 Milne, "Trump's Baltic Shift," 1.

260 The European Reassurance Initiative (ERI) refers to the Department of Defense (DOD) fund that was begun in the aftermath of the Crimea crisis in June 2014. The ERI funds and supports U.S. defensive measures, including bilateral and multilateral military training, exercises, deployments, and investments in Central and Eastern Europe, especially in Bulgaria, the Czech Republic, Estonia, Georgia, Latvia, Lithuania, Moldova, Poland, Romania, Slovakia, and Ukraine; the purpose of the ERI is to reassure America's Allies and partners of U.S. resolve and commitment to their security. (The White House, "Fact Sheet: European Reassurance Initiative and Other U.S. Efforts in Support of Allies and Partners," June 3, 2014, https://www.whitehouse.gov/the-press-office/2014/06/03/fact-sheet-european-reassurance-initiative-and-other-us-efforts-support-, 1, 3).

261 "Fact Sheet: European Reassurance," 1.

262 Milne, "Trump's Baltic Shift," 1.

263 "Trump Presidency 'Would Make World Less Safe'—Ex NATO Boss," BBC, August 15, 2016, http://www.bbc.com/news/election-us-2016-37090988.

If the publics and presidential frontrunners in major NATO nations are unwilling to uphold national commitments under the Washington Treaty after an armed attack on an Ally, what does this waning support imply for their resolve to do so in reply to a perceived lesser assault in cyberspace? Waning public support for honoring Article 5 commitments may signify an even lower willingness to meet NATO's collective defense obligations in response to an act of terrorist or state-sponsored cyber aggression. Some public opinion polls suggest that if a cyber threat met the threshold of an armed attack, NATO might be less prepared politically to invoke Article 5 than in a case of conventional military aggression. While polling is an important tool in political decision making, in practice governments take many factors in addition to public surveys into account in deciding whether and how to use force. Declines in political will and public support for NATO's collective defense principle in some Allied member states have left NATO minimally prepared to respond effectively to major acts of cyber aggression against one or more of its members, particularly when that response necessitates the use of military force. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 1 in political will.

E. CRISIS MANAGEMENT

As this thesis has shown, NATO has evolved organizationally to address burgeoning threats in the digital dimension; it has created multiple cyber response agencies, centers, and teams and updated its policies to reflect heightened cybersecurity standards. From an organizational and cybernetic standpoint, NATO is highly prepared for cyberwar. Yet if cyber aggression turned kinetic against an Ally, would the Alliance be effective in conducting a combined military campaign? The Alliance has led multiple counter-piracy missions, including Operations Allied Protector and Ocean Shield, support missions for the Africa Union, peace-time operations such as the Baltic Air Policing (BAP) mission, and humanitarian assistance and relief activities for Pakistan, Portugal, Turkey, Ukraine, and the United States.[264] Yet, NATO has conducted only four major

264 "Operations and Missions: Past and Present," NATO, July 12, 2016, http://nato.int/cps/en/natohq/topics_52060.htm?selectedLocale=en, 3, 6.

combat operations as a coalition. An examination of these four operations is the next subject of this thesis.

1. Bosnia: Operation Deliberate Force

NATO conducted its first-ever combat operation from August 30, 1995 to September 20, 1995 within the former Yugoslavia.[265] Although the Alliance conducted an arms embargo and a no-fly zone in the Balkan region as early as July 1992, NATO did not engage in major strike operations against Serbia until three years later.[266] After the July 1995 massacre in Srebrenica, in which Bosnian Serbs slaughtered 7,079 Bosnian Muslim men and boys within a UN safe zone, the UN requested NATO intervention to assist the efforts of the United Nations Protection Force (UNPROFOR).[267] Under the auspices of United Nations Security Council Resolutions (UNSCRs) 781, 816, and 836, NATO's air and artillery campaign aimed to bring peace and stability to the former Yugoslavia, which had been entrenched in an ethnic civil war since 1991.[268] After just three weeks, NATO successfully suppressed and overwhelmed the air defenses of the Bosnian Serbs.[269] Through its judicious employment of airpower, NATO was internationally credited with effectively ending the Bosnian War.[270]

During the campaign, NATO employed various electronic technologies and information resources within the cybernetic domain. In addition to maintaining secure lines of communication to facilitate command and control (C2) among Allied forces, NATO relied on satellite and IT communications networks to integrate its air defense systems and manage all air activities and strike engagements.[271] The Alliance also used

---

265 Robert C. Owen, ed., *Deliberate Force: A Case Study in Effective Air Campaigning*, Maxwell Air Force Base, Alabama: Air University Press, 2000, http://www.au.af.mil/au/awc/awcgate/au/owen.pdf, xvii.

266 Yost, *NATO's Balancing Act*, 127.

267 Ivo H. Daalder, "Decision to Intervene: How the War in Bosnia Ended," Brookings Institution, December 1, 1998, https://www.brookings.edu/articles/decision-to-intervene-how-the-war-in-bosnia-ended/, 2.

268 Owen, *Deliberate Force: A Case Study*, xix, 39.

269 Owen, *Deliberate Force: A Case Study*, xxi.

270 Ryan C. Hendrickson, "Crossing the Rubicon," *NATO Review*, 2005, http://www.nato.int/docu/review/2005/issue3/english/history.html, 1.

271 Owen, *Deliberate Force: A Case Study*, 50, 52, 58.

electronic and signals intelligence methods to intercept Bosnian Serb communications and target various telecommunications and radar facilities, even severing links between the Bosnian Serbs' headquarters and the capital at Belgrade.[272] Moreover, Allied forces deployed electronic combat assets to suppress, degrade, and/or destroy ground-based emitters for enemy air defense systems.[273] NATO also employed advanced sensor technologies to conduct intelligence, surveillance, and reconnaissance (ISR) operations.[274] Yet while the cyber domain played a distinct role in most aspects of mission planning, targeting, communications, and execution, it was not the domain targeted by NATO's adversaries. For this reason, cyber defense and security played negligible roles for the Allies during the conflict.

Throughout the campaign, NATO had several objectives. The Alliance had ultimately hoped that its military intervention would pressure Serbian leader Slobodan Milosevic to concede not only militarily but politically.[275] The operation's defined objectives were (1) to deter and reduce attacks within UN safe zones (Bosnian cities), (2) to force the Bosnian Serbs to remove heavy weapons from the total exclusion zone around Sarajevo, (3) to ensure freedom of movement for UN and non-governmental organizations (NGOs), and (4) to keep the Sarajevo airport open.[276]

These objectives came with challenges. Coordination between the bureaucratic command and control (C2) structures of NATO and the UN often slowed down decision making, which put tactical forces on the ground at risk.[277] In addition, the divergent interests and political dispositions of NATO members, like Germany (which favored the Croats), Greece (which favored the Serbs), and Turkey (which favored the Bosnians) threatened Allied consensus.[278] Another variable that factored into the organization's

---

[272] Owen, *Deliberate Force: A Case Study*, 147, 191.

[273] Owen, *Deliberate Force: A Case Study*, 210.

[274] Owen, *Deliberate Force: A Case Study*, 225.

[275] Owen, *Deliberate Force: A Case Study*, xix, xx.

[276] Owen, *Deliberate Force: A Case Study*, 44.

[277] Owen, *Deliberate Force: A Case Study*, 59.

[278] Owen, *Deliberate Force: A Case Study*, 17.

wartime calculus was the role that each NATO member preferred to play. Dissimilar strategic visions, like those of the United States and Germany (which favored a strong military intervention) and those of the UK and France (which favored a peacekeeping role) complicated the strategic scope of NATO's involvement.[279] While the European Allies had a large political function in the planning and execution of the effort, they were less involved militarily.[280] The United States comprised about 45 percent of forces assigned and flew nearly 66 percent of the air missions, totaling 2,318 sorties.[281]

Some critics assert that the unanimity component of the consensus-driven North Atlantic Council (NAC) delayed NATO's large-scale intervention in the Balkan region until 1995.[282] Yet, once the Alliance actually intervened, it was instrumental to the establishment of regional stability and the NATO-led Implementation Force (IFOR), which replaced UNPROFOR.[283] Through constant intra-Alliance cooperation and military coordination with the UN, NATO ultimately met its military objectives in Operation Deliberate Force, setting the geo-strategic stage for the future achievements of the Dayton Peace Accords.[284] By 1996, NATO established the Stabilization Force (SFOR) to assist with the country's reconstruction effort and implement necessary regional security measures.[285] While NATO ended the SFOR mission and transferred its stabilization responsibilities to the EU in December 2004,[286] questions about the effectiveness of its stabilization efforts remain. Although the Dayton Accords brought the Bosnian ethnic conflict to a close, hostilities later re-emerged in another region of the Balkans—Kosovo.

---

279 Owen, *Deliberate Force: A Case Study*, 17.

280 Owen, *Deliberate Force: A Case Study*, xviii.

281 Owen, *Deliberate Force: A Case Study*, 204; John A. Tirpak, ed., "Deliberate Force," *Air Force Magazine*, October 1997, http://www.airforcemag.com/magazinearchive/documents/1997/october%201997/1097deliberate.pdf, 39.

282 Hendrickson, "Crossing the Rubicon," 1, 3.

283 Hendrickson, "Crossing the Rubicon," 1, 3.

284 Tirpak, "Deliberate Force," 43.

285 "Peace Support Operations in Bosnia and Herzegovina," NATO, September 7, 2015, http://nato.int/cps/en/natohq/topics_52122.htm?selectedLocale=en, 1.

286 "Peace Support Operations in Bosnia and Herzegovina," 1.

2. Kosovo: Operation Allied Force

Before cyber aggression was launched against Estonia (2007), Georgia (2008), and Ukraine (2013-present), the Alliance as a whole experienced its first string of major cyber attacks during the Kosovo conflict.[287] From March 23, 1999 to June 10, 1999, NATO conducted a 78-day air-strike operation in response to Serbian President Slobodan Milosevic's ethnic cleansing campaign.[288] The genocide against Kosovar Albanians left over 250,000 dead and hundreds of thousands of Kosovar refugees displaced.[289]

During the Kosovo mission, Serbian hackers and Yugoslav Army forces disrupted NATO's digital infrastructure—including its websites, servers, and email communications.[290] By employing various intrusion techniques, including the Packet Internet Groper (PING) bombardment strategy that sent constant pings and messages to NATO's servers, hackers were able to overwhelm and take offline key NATO websites.[291] Due to the disruptions, NATO's public affairs website was inoperable for several days, which delayed the Alliance in communicating its version of events to the public.[292] Serbian hackers also attacked NATO's email infrastructure using the Happy 1999 macro self-spreading virus, which worked by preventing the Allies' computers from properly interfacing with the Internet and crashing their screens with a fireworks animation.[293] Additionally, hackers from all over the world, including China and Russia, targeted the servers of Allied governments and militaries, including those of the United

---

287 Yost, *NATO's Balancing Act*, 44.

288 Gregory Ball, "Operation Allied Force," August 23, 2012, http://www.afhso.af.mil/topics/factsheets/factsheet.asp?id=18652, 1.

289 Ball, "Operation Allied Force," 1.

290 Yost, *NATO's Balancing Act*, 44.

291 Dan Verton, "Serbs Launch Cyber Attack on NATO," FCW, April 4, 1999, https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx, 1; Jason Healey, "Cyber Attacks Against NATO, Then and Now," *The Atlantic Council*, September 6, 2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now, 1.

292 *The Evolution of U.S. Cyber Power*, The Armed Forces Communications and Electronics Association, accessed August 13, 2016, http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf, 19, 21.

293 Verton, "Serbs Launch Cyber Attack," 1.

States.[294] For example, during Operation Allied Force, White House and Department of Defense (DOD) websites were hacked and defaced.[295] NATO also struggled with transmitting digital data through its joint data network.[296] Because the Allies operated using different transmission systems and messaging formats, NATO had to resort to manual transfers of tactical digital information.[297] The lack of interconnectivity and compatibility of the Allies' tactical data systems increased manpower requirements, slowed operational tempo, and enlarged the potential for human error during each phase of its air-strike operation.[298]

The electronic problems and cyber attacks encountered throughout Operation Allied Force dealt coalition forces their first cybernetic blow and forced NATO to take a hard look at its internal cyber defense protocols. In fact, the Alliance took the first steps to publicly address the issues concerning its cyber policies and defenses during the Prague and Bucharest Summits of 2002 and 2008, respectively.[299] According to cyber analyst Jason Healey, "It was partially the 1999 incidents during Allied Force that drove NATO's leadership at the 2002 Prague Summit to create the NATO Computer Incident Response Capability (NCIRC)."[300]

From the onset, Operation Allied Force also experienced challenges outside of cyberspace; many of these hurdles derived from intra-alliance tensions and legitimacy issues. Unlike in Operation Deliberate Force, the NATO Allies in Operation Allied Force acted without an official UN Security Council (UNSC) mandate, which deprived the Alliance of credibility in the eyes of its international partners.[301] In fact, UN Secretary General Kofi Annan criticized NATO for undermining the institution's primacy as the

294 *Evolution of U.S. Cyber Power*, 19; Healey, "Cyber Attacks Against NATO," 1.

295 *Evolution of U.S. Cyber Power*, 19; Healey, "Cyber Attacks Against NATO," 1.

296 "Kosovo/Operation Allied Force After Action Report," Department of Defense, Report to Congress, January 31, 2000, 49.

297 "Kosovo/Operation Allied Force After Action Report," 49.

298 "Kosovo/ Operation Allied Force After Action Report," 50.

299 Yost, *NATO's Balancing Act,* 44.

300 Healey, "Cyber Attacks Against NATO," 1.

301 "NATO and Operation Allied Force," Polity, accessed March 24, 2016, https://www.polity.co.uk/up2/casestudy/NATO_and_Operation_Allied_Force.pdf, 1, 4.

"sole source of legitimacy" (aside from Article 51 of the UN Charter) for the employment of force.[302] Yet, if NATO had made formal attempts through the UNSC for authorization of a military intervention, any decision would have been vetoed by China and Russia, which still do not recognize Kosovo's independence today.[303] According to then Secretary of State Madeleine Albright, any decision by the world's top liberal democracies, which were represented in the NAC, held more legitimacy than a legal decision made by a five-member council including two repressive regimes.[304] While the Alliance set a potentially dangerous precedent for unilaterally undertaking offensive actions against a sovereign nation, it demonstrated international activism in the face of irrefutable evidence of genocide.[305]

The Alliance also applied lessons learned from Deliberate Force throughout its Kosovo operation. For example, NATO took important measures to minimize decision paralysis, which stemmed from the need for consensus.[306] By leaving subordinate committees out of the NAC's decision-making process and ceding to then Secretary General Javier Solana decisions to execute a pre-approved airstrike plan, NATO was able to rapidly translate strategy into tactical actions on the ground.[307] While the first two phases of the operation encountered setbacks due to poor weather, topography, and coordination challenges, NATO's third phase of strategic air strikes (and other factors) compelled Milosevic to withdraw his forces from Kosovo.[308]

Throughout the campaign, NATO's political and military objectives were (1) to put an end to the Serbian-led violence, oppression, and military activities in Kosovo, (2) to compel Serbian military and paramilitary forces to withdraw from Kosovo, (3) to station an international military presence, (4) to ensure that displaced persons and

302 "NATO and Operation Allied Force," 1, 4.

303 "NATO and Operation Allied Force," 2–3.

304 "NATO and Operation Allied Force," 2–3.

305 "NATO and Operation Allied Force," 1; Michel, "NATO Decision Making," 2.

306 Michel, "NATO Decision Making," 3.

307 Michel, "NATO Decision Making," 3.

308 Ball, "Operation Allied Force," 1.

refugees were safely re-settled with access to humanitarian NGOs, and (5) to establish a political settlement for Kosovo that was consistent with international law.[309] By June 10, 1999, NATO had fulfilled its objectives and signed a Military Technical Agreement with the Federal Republic of Yugoslavia.[310] The Alliance also deployed an international contingent of civilian workers and security personnel for its Kosovo Force (KFOR) mission to promote peace and stability.[311]

Although the KFOR mission has been in place since 1999 and has maintained between 50,000 troops (at its peak) and 4,687 troops (at its current level), Kosovo still remains a cradle of instability for Europe.[312] In fact, many scholars believe that with Kosovo's unremitting economic, political, and multiethnic hurdles, the international intervention in Kosovo by NATO, the EU, and other organizations, has yet to yield the success envisaged at the outset. Nonetheless, while stability operations remain the most challenging aspect of NATO's post-conflict role in Kosovo, the Alliance was decisively effective during its military campaign. In 2008, all of NATO's basic objectives were met. Kosovo legally declared independence in February 2008 and today is formally recognized by 111 of 193 UN member states and most NATO and EU members.[313] At the end of its operations, NATO had taken extraordinary efforts to minimize collateral damage, completing over 38,000 sorties with zero Allied fatalities.[314] These military achievements help explain why Operation Allied Force is regarded as one of NATO's greatest operational successes.

---

309 "The Kosovo Air Campaign (Archived): Operation Allied Force," NATO, October 13, 2015, http://www.nato.int/cps/en/natohq/topics_49602.htm, 3.

310 "Kosovo Air Campaign (Archived): Operation Allied Force," 3.

311 "Kosovo Air Campaign (Archived): Operation Allied Force," 3.

312 "Kosovo Force (KFOR) Key Facts and Figures," May 2015, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_05/20150508_1505-kfor-placemat.pdf, 1; Yost, *NATO's Balancing Act*, 132.

313 Neil MacDonald, James Blitz, and Michael Steen, "Kosovo Ruling Seen as Boon to Separatists," *Financial Times*, July 22, 2010, http://www.ft.com/cms/s/0/d4da3fa2-959d-11df-a2b0-00144feab49a.html#axzz4Jm990pTN, 1; "Who Recognized Kosovo as an Independent State?," accessed March 25, 2016, http://www.kosovothanksyou.com/.

314 Ball, "Operation Allied Force," 1.

3. Afghanistan: International Security Assistance Force (ISAF) Mission

After the September 11 terrorist attacks on the United States, NATO forces assumed the lead in collective security efforts in Afghanistan from December 20, 2001 to December 28, 2014.[315] Upon Afghanistan's request and under the auspices of nine UN Security Council Resolutions (UNSCRs), including 1386, 1413, 1444, 1510, 1563, 1623, 1707, 1776, and 1833, NATO was assigned the daunting task of providing security for the UN-led efforts to bring stability to a region in which ethnic, sectarian, tribal, and ideology-driven factions have competed for power for thousands of years.[316]

Before and during NATO's mission, cyberspace played a distinct role for both the Alliance and its adversaries. Al Qaeda—the global terrorist organization founded and sponsored by Osama bin Laden—began employing Internet tools to advance its political and military agendas in the 1980s.[317] By 2001, the organization was training many of its operatives in sophisticated hacking, data encryption, and coding techniques.[318] With chat rooms, website forums, online magazines, and social media sites like Twitter, Al Qaeda's Electronic Army was able to disseminate information, rationalize its activities ideologically, relay critical intelligence, and upload propaganda videos for recruitment.[319] Additionally, Al Qaeda frequently conducted "electronic jihad" against the West by orchestrating cyber attacks against NATO and U.S. cyber targets.[320] Strong evidence also suggests that Al Qaeda coordinated the September attacks in cyberspace.[321] In fact, Al Qaeda operatives collected a majority of the intelligence on U.S. targets cybernetically via open source publications and communicated the information using

315 "ISAF's Mission in Afghanistan (2001-2014) (Archived)," NATO, September 1, 2015, http://www.nato.int/cps/en/natohq/topics_69366.htm, 1.

316 "ISAF Mandate," NATO, last modified April 29, 2009, http://www.nato.int/isaf/topics/mandate/, 1.

317 *Terror Goes Cyber: The Cyber Strategies and Capabilities of Al Qaeda, ISIS, Al Shabaab, and Boko Haram*, Bat Blue, April 2015. http://www.batblue.com/wp-content/uploads/2015/04/BatBlueReport_TerrorGoesCyber.pdf, 4.

318 *Terror Goes Cyber*, 4–5.

319 *Terror Goes* Cyber, 4–5; Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyber-planning.' *Parameters*, Spring 2003, http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf, 115.

320 *Terror Goes Cyber*, 5.

321 Thomas, "Al Qaeda and the Internet," 112, 118.

encrypted electronic messages.[322] Throughout the NATO mission in Afghanistan, Al Qaeda and other non-state actors have also conducted cyber attacks using malicious viruses and malware; since the inception of ISAF, these types of cyber incidents on Afghanistan's digital infrastructure have increased exponentially.[323]

To confront the cybernetic challenges posed by Al Qaeda, NATO—with the United States in the lead—has employed various tools. During the mission in Afghanistan, the United States Government contracted cyber experts to lead offensive cyber operations.[324] Specifically, the U.S. DOD employed teams skilled in computer network operations, especially cyber tracking, analysis, exploitation, and attack to support the execution of the mission in Afghanistan and the political objectives of the United States and NATO.[325] Alongside the United States' offensive cyber operations, NATO led cybersecurity training to reinforce the digital defenses of the country. In 2012 NATO, under the auspices of the Science for Peace and Security (SPS) Program, established a 10-day cyber defense training course for Afghan students.[326] The course provided Afghan network administrators with critical skills training on cyber defense measures, coding, threat identification, and threat response protocols to help Afghanistan develop an institutional cyber defense capability.[327]

The ISAF mission's main objectives were (1) to conduct security and stability operations in Afghanistan, (2) to help develop and train an Afghan National Security Force (ANSF) and an Afghan National Army (ANA), (3) to identify reconstruction needs, (4) to support the Afghan government with disarming illegally armed groups, (5) to provide intelligence-sharing and information support to the Afghan government and to

322 Thomas, "Al Qaeda and the Internet," 112, 118.

323 "Afghan Managers Train in Cyber Defense," NATO, May 21, 2012, http://www.nato.int/cps/en/natolive/news_86990.htm, 2.

324 Marc Ambinder, "Cyber Attacks in Afghanistan, *The Week*, April 2, 2013. *http://theweek.com/articles/466007/cyberattacks-afghanistan*, 1.

325 Ambinder, "Cyber Attacks in Afghanistan," 1–2.

326 "Afghan Managers Train in Cyber Defense," 1–2.

327 "Afghan Managers Train in Cyber Defense," 2.

counter-narcotics efforts, and (6) to assist with humanitarian operations.[328] The Alliance encountered problems achieving many of these objectives from the onset.

NATO's efforts to build unity, military professionalism, and civic mindedness within the Afghan forces became nearly an insuperable task due to potent cultural and provincial identities. Thirteen years after its original mandate, ISAF never achieved its primary goal of building an effective security apparatus in the country.[329] The rise of the Islamic State of Iraq and the Levant (ISIL) and factional clashes with the Taliban in the region complicated the already chaotic security situation.[330] Although NATO succeeded in enabling Afghanistan to make some advancements in economic development, education, governance, and human rights,[331] the nation may still be generations away from transitioning into a stable, secure, and united country. To date, since 2001 the war in Afghanistan has yielded 3,515 coalition fatalities and 92,000 Afghan fatalities, including 26,000 Afghan civilians.[332] While NATO officially transferred responsibility for security to the Afghan forces in December 2014, the Alliance has continued its mission under a new name with Resolute Support, which began on January 1, 2015.[333] NATO's ISAF mission was one of the largest coalitions in history; at its height it had 150,000 troops deployed from approximately 50 countries.[334] While the mission enhanced interoperability among Allied militaries,[335] it was one of the costliest and least effective initiatives undertaken by the Alliance.

---

328 "ISAF Mandate," 1.

329 "ISAF's Mission in Afghanistan (2001-2014) (Archived)," 1.

330 Mujib Mashal and Andrew E. Kramer, "Russia Pulls Back from Cooperating with U.S. on Afghanistan," *New York Times*, February 20, 2016, http://www.nytimes.com/2016/02/21/world/asia/russia-pulls-back-from-cooperating-with-us-on-afghanistan.html?_r=0, 4.

331 "Wales Summit Declaration on Afghanistan issued by Heads of State and Government of Allies and their International Security Assistance Force (ISAF) Troop Contributing Partners," NATO, September 4, 2014, http://www.nato.int/cps/en/natohq/news_112517.htm, 1–2.

332 "Operation Enduring Freedom," iCasualties, accessed March 25, 2016, http://icasualties.org/oef/, 1; "Costs of War," Watson Institute for International and Public Affairs, last modified March 2015, http://watson.brown.edu/costsofwar/costs/human/civilians/afghan, 2.

333 "ISAF's Mission in Afghanistan (2001-2014) (Archived)," 1.

334 Jamie Shea, "Keeping NATO Relevant," *Carnegie Endowment for International Peace*, (2012), 3.

335 "ISAF's Mission in Afghanistan (2001-2014) (Archived)," 2.

4. Libya: Operation Unified Protector

From March 20, 2011, to October 31, 2011, NATO intervened in the Libyan Civil War on humanitarian grounds.[336] With the United States pushing for a European-led coalition, the Alliance began its seven-month combat operation to stop the Muammar Gaddafi regime from systematically killing members of the civilian population.[337] With UN approval under UNSCRs 1970 and 1973, NATO established a no-fly zone, enforced an arms embargo, conducted air and naval strikes, and prevented large-scale civilian losses in Libya.[338]

During Operation Unified Protector, the Alliance experienced only three significant cyber attacks.[339] The first cyber intrusion allegedly extracted and released sensitive data from the NATO server, while the second attack occurred on a NATO affiliate's website and publicized the usernames and passwords of the site's 12,000 registered users.[340] In the third cyber intrusion, hackers used malicious email software to extract unclassified information from a host computer in the Norwegian military.[341] While these data breaches were serious, they were mild in comparison to the deluge of denial-of-service attacks that NATO experienced during the Kosovo campaign.[342] NATO was careful not to repeat the mistakes in cyberspace that it had made nearly twelve years prior.[343] It should be recalled that between 1999 and 2011, the Alliance created its first cyber strategy, outfitted its organizational structure with numerous cybernetic elements,

---

336 "NATO and Libya (Archived)," NATO, November 9, 2015, http://www.nato.int/cps/eu/natohq/topics_71652.htm, 1.

337 Jeffrey Goldberg, "The Obama Doctrine," *The Atlantic*, April 2016, http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/, 16.

338 Karl P. Mueller, ed., "Precision and Purpose: Airpower in the Libyan Civil War," 2015, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR676/RAND_RR676.pdf, 25, 51, 58, 133.

339 Healey, "Cyber Attacks Against NATO," 1.

340 Healey, "Cyber Attacks Against NATO," 1.

341 "Norway Army Says Faced Cyber Attack after Libya Bombing," *ABS/ CBN News*, May 19, 2011, http://news.abs-cbn.com/global-filipino/world/05/19/11/norway-army-says-faced-cyber-attack-after-libya-bombing, 1.

342 Healey, "Cyber Attacks Against NATO," 1.

343 *Evolution of U.S. Cyber Power*, 23.

and bolstered its network security and response capabilities.[344] Due to the changes made to NATO's cyber defense structure, the Alliance's cyber apparatus was more prepared for the network breaches it suffered during the Libyan campaign.[345]

NATO's military objectives during the Libyan intervention were (1) to stop the attacks and threats of attack against civilians, (2) to compel the Gaddafi regime to withdraw its forces, and (3) to ensure freedom of movement for all humanitarian efforts within Libya.[346] Allied forces accomplished these objectives by enforcing a maritime arms embargo in the Mediterranean, imposing a no-fly zone, and conducting air and naval strikes against regime forces.[347] By the end of October 2011, NATO was praised for a successful operation that had involved over 26,000 sorties, 250 aircraft, 21 ships, and 8,000 military personnel from Allied and partner nations.[348] Operation Unified Protector had ended with an outward appearance of civilian lives protected, Libya liberated, and the repressive Gaddafi regime overthrown.

Yet in 2012, following NATO's immediate military withdrawal, the internal security situation quickly deteriorated.[349] Inter-militia fighting and jihadist activity in Libya produced frequent attacks on civilian-populated areas, including the Red Cross offices in Tripoli and Benghazi, the Tunisian Consulate, and the Tripoli Airport.[350] On September 11, 2012, the most infamous of these attacks occurred, leaving Ambassador Christopher Stevens and three other Americans dead.[351] Today, the security quagmire in Libya has deepened to the point that it has been described by President Obama as "a

---

344 For additional background, see Chapter V: NATO's Level of Preparedness, Section A, Cyber Strategy and Section B, Cyber Cooperation.

345 Healey, "Cyber Attacks Against NATO," 1.

346 Florence Gaub, "The North Atlantic Treaty Organization and Libya: Reviewing Operation Unified Protector," *The Letort Papers*, U.S. Army War College Press: Carlisle, PA, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub1161.pdf, 19.

347 "Operations and Missions: Past and Present," 8.

348 "NATO and Libya (Archived)," 7.

349 Gaub, "The North Atlantic Treaty Organization and Libya," 28.

350 Gaub, "The North Atlantic Treaty Organization and Libya," 28.

351 Gaub, "The North Atlantic Treaty Organization and Libya," 28.

mess" and by others as "an abject failure."[352] The country now has hundreds of decentralized militias that are fragmented along ideological, geographical, religious, and ethnic lines.[353] These factions have disparate interests and operate autonomously, creating societal schisms that have resulted in the disintegration of state institutions, the growth of jihadism, and the slaughter of innocent civilians caught in the middle.[354] Libya's problems with poor governance, terrorism, and rebel militias have transformed it into a safe haven for violent extremist groups to operate and coordinate terrorist attacks.[355] The United States and NATO view Operation Unified Protector as a $1 billion lesson learned, which has kept the Alliance (so far) out of other Middle Eastern conflicts, including the Syrian Civil War.[356]

During each of NATO's four major combat operations, the Alliance experienced many operational achievements but also some significant long-term setbacks. Problems with the consensus model during Operation Deliberate Force delayed the Allies' involvement for several years, thereby protracting the war in Bosnia and multiplying the number of casualties that followed under UNPROFOR leadership. Moreover, it was only after the occurrence and subsequent international condemnation of one of the most overt cases of genocide (within the Bosnian Muslim enclave of Srebrenica) that NATO (via UN mandates) was compelled to act decisively.[357] Once NATO intervened in the crisis, the Allies achieved nearly instantaneous success. By employing robust military force, NATO was able to pressure the Serbian government to negotiate a peace settlement, which helped steer the Balkan geopolitical landscape toward greater stability. Yet, the

352 Goldberg, "Obama Doctrine," 16–17*;* Derek Chollet, Ben Fishman, and Alan J. Kuperman. "Who Lost Libya? Obama's Intervention in Retrospect," *Foreign Affairs,* May/June 2015, https://www.foreignaffairs.com/articles/libya/2015-04-20/who-lost-libya, 1.

353 Barak Barfi, "What's Really Holding Libya Back," *NATO Review,* 2014, http://www.nato.int/docu/review/2014/Also-in-2014/Security-political-problems-Libya/EN/index.htm, 1.

354 Barfi, "What's Really Holding Libya Back," 1.

355 Ewen MacAskill, "International Force of 5,000 Prepares for Libya Deployment," *The Guardian,* March 7, 2016, http://www.theguardian.com/world/2016/mar/07/international-force-ready-for-libya-deployment-as-terror-threat-fears-grow, 1.

356 Goldberg, "Obama Doctrine," 17.

357 Daalder, "Decision to Intervene," 3.

peace attained through the Dayton Accords was short-lived, as five years later, NATO had to intervene once again in the Balkan region with Operation Allied Force.

While NATO was operationally effective and more decisive during Operation Allied Force in comparison to Deliberate Force, the Alliance failed to foster a stable post-war environment free of ethnic tensions. Today, both Bosnia-Herzegovina and Kosovo remain divided along ethnic lines.[358] The Dayton Peace agreement, led by the United States but involving several states in the Peace Implementation Council, further institutionalized religious and ethnic divisions through the creation of separate ethno-federations[359] for Bosnian Croats, Muslims, and Serbs.[360] In both Kosovo and Bosnia-Herzegovina, ethnic identity remains salient, and some of the same forms of ethno-nationalism, which served to polarize society during the crises, still saturate Balkan politics today.[361] While NATO does not share full blame for the unsatisfactory conditions in the Balkans, the Allies' policy failures before and during the Dayton Accords contributed to the stagnation and in some cases retraction of political progress in Bosnia and Kosovo. Some critics hold that it is only a matter of time before another crisis in the region develops.[362]

NATO's Strategic Concept defines "crisis management" as military and political measures taken to "address the full spectrum of crises—before, during, and after conflicts."[363] According to the Alliance, the purpose of this core capability is to "help

---

358 "Bosnia-Herzegovina Profile-Overview," BBC, March 25, 2016. http://www.bbc.com/news/world-europe-17211937, 3; Lenard Cohen, "Nationalism, the Kosovo Crisis, and Political Change in Serbia," July 7, 2011, https://www.wilsoncenter.org/publication/164-nationalism-the-kosovo-crisis-and-political-change-serbia, 1.

359 An ethno-federation is a federalized system comprised of sub-organizational entities, which 1) govern and divide territory according to ethnic classifications, 2) adhere to a constitution, and 3) have autonomy in at least one political domain. (Henry Hale, "Divided We Stand: Institutional Sources of Ethno-federal Survival and Collapse," *World Politics* 56, no. 2 (January 2004): 167). The former Yugoslavia was divided into six ethno-federal republics: Bosnia-Herzegovina, Croatia, Macedonia, Montenegro, Serbia, and Slovenia.

360 Hale, "Divided We Stand," 165.

361 Cohen, "Nationalism, the Kosovo Crisis, and Political Change in Serbia," 1; Jonathan S. Landay, "20 Years after War Began, Bosnia Grows More Divided," *McClatchy Newspapers,* April 25, 2012, http://www.mcclatchydc.com/news/nation-world/world/article24728359.html, 5.

362 Landay, "20 Years after War Began," 5.

363 *Strategic Concept*, 7–8.

manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts [and] to stop ongoing conflicts where they affect Alliance security."[364] Based upon these definitions, some analysts would assert that Afghanistan and Libya are in worse socio-political conditions than they were before NATO's involvement. Multiple international organizations alongside NATO—above all the UN and in some cases the EU—bear political responsibility for the consequences of these operations. Instead of improving the security situation in Afghanistan and Libya, NATO's efforts (in conjunction with those of several other organizations) helped entrench the affected states in deeper conflict. NATO, especially in Bosnia, Kosovo, and Libya, excelled in putting an immediate end to the hostilities, but was unsuccessful (in the company of many other international organizations) in establishing a stable and enduring peace.

In all, NATO's crisis management measures have failed to adequately address "the full spectrum of crises"[365] that have developed since the early 1990s. Yet, it should be noted that all four NATO-led operations were expeditionary operations in support of collective security. This thesis makes the assumption that the Alliance would be responding to an act of cyber aggression. In the case of an act of cyberwar that triggered an Article 5 invocation, NATO would probably be more effective in managing the threat cybernetically than with a conventional crisis management approach involving combat measures. NATO's crisis management procedures and operational performance have minimally prepared the Alliance to effectively manage a cyberwar that evolves into a conventional wartime scenario. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 1 in crisis management.

F. DEFENSE SPENDING

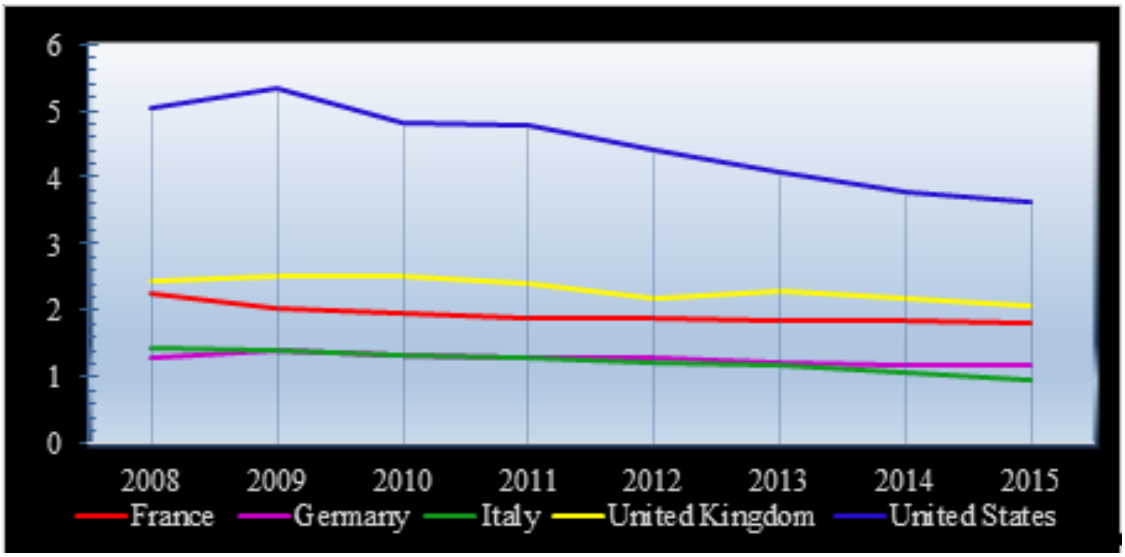
This section evaluates whether NATO—under the de facto economic leadership of France, Germany, Italy, the UK, and the United States—is prepared to respond to cyber aggression that rises to the level of Article 5. Only the defense investment policies

364 *Strategic Concept*, 8.

365 *Strategic Concept*, 7–8.

of NATO's most influential members—France, Germany, Italy, the UK, and the United States—have been assessed because of the level of economic strength they bring to bear within the Alliance. NATO members face budgetary and policy constraints that present various challenges to overall readiness. The analysis begins with a review of national defense spending patterns. Figure 1 shows the relative decline in defense spending for France, Germany, Italy, the UK, and the United States between 2008 and 2015:

Figure 1. Defense Expenditure as a Percentage of Gross Domestic Product[366]



1. France

In 2006, NATO's 28 Allies pledged to spend at least 2 percent of their gross domestic product (GDP) on national defense.[367] At the 2014 Wales Summit, NATO declared that any Allies whose current defense expenditure was below this 2 percent guideline would "halt any decline in defense expenditure, aim to increase defense expenditure in real terms as GDP grows, [and] aim to move toward the 2% guideline within a decade with a view to meeting their NATO Capability Targets and filling

366 Adapted from "Defense Expenditures of NATO Countries (2008-2015)," NATO, January 28, 2016, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160129_160128-pr-2016-11-eng.pdf#page=6, 6.

367 "Funding NATO," 1.

NATO's capability shortfalls."[368] According to this pronouncement, NATO members have until 2024 to increase their defense spending, but there is currently no firm deadline for the Allies to meet the 2 percent of GDP spending standard. Today, the nations that adhere to the 2 percent guideline are Estonia, Greece, Poland, the UK, and the United States.[369] At the 2016 Warsaw Summit, NATO announced that 10 Allies met another NATO defense standard—to spend more than 20 percent of their defense budgets on major equipment.[370]

While France fails to meet the agreed 2 percent minimum, the country is still ranked as one of the top 10 national defense spenders in the world.[371] As the world's sixth largest and Europe's third largest economy, France spent close to $44 billion on defense in 2015.[372] In 2014, France invested over $1 billion to upgrade its cyber defenses, network monitoring capabilities, and system encryption competencies in order to improve the digital critical infrastructure in its financial and defense sectors.[373] According to the government's 2013 *French White Paper: Defense and National Security*, France is also allocating €364 billion (roughly $400 billion) between 2014 and 2025 to help meet its three national defense priorities of protection, deterrence, and intervention.[374]

In spite of these spending initiatives, France's defense spending as a percentage of GDP has declined steadily since 2008.[375] Per Figure 1, France spent about 1.8 percent of

---

368 "Wales Summit Declaration," par. 14.

369 Naftali Bendavid, "Just Five of 28 NATO Members Meet Defense Spending Goal, Report Says," *The Wall Street Journal*, June 22, 2015, http://www.wsj.com/articles/nato-calls-for-rise-in-defence-spending-by-alliance-members-1434978193, 1.

370 "Warsaw Summit Communiqué," par. 34.

371 "Defense Budget by Country," Global Firepower, accessed March 11, 2016, http://www.globalfirepower.com/defense-spending-budget.asp, 1.

372 "Defense Expenditures of NATO Countries," 7; Prableen Bajpai, "The World's Top Economies," Investopedia, last modified July 18, 2016, http://www.investopedia.com/articles/investing/022415/worlds-top-10-economies.asp, 2.

373 "France to Invest 1 Billion Euros to Update Cyber Defenses," *Reuters*, February 7, 2014, http://www.reuters.com/article/france-cyberdefence-idUSL5N0LC21G20140207, 1.

374 *French White Paper: Defense and National Security*, Presidency of the French Republic, 2013, http://www.rpfrance-otan.org/White-Paper-on-defence-and, 7, 84.

375 "Defense Expenditures of NATO Countries," 6.

GDP on defense in 2015—down 35 percent from its defense expenditures in 2008.[376] Additionally, France's rising debt levels could pose a significant concern in the near future. With its debt to GDP ratio hovering above 95 percent, rising domestic discontent over the nation's fiscal priorities and defense appropriations could compel national leaders to reexamine defense spending requirements.[377]

Despite fiscal constraints and downward spending trends, domestic and geopolitical crises sometimes compel state actors to reevaluate past budgetary decisions. As with the decisions following the January 2015 *Charlie Hebdo* attacks, the November 2015 terrorist attacks in Paris compelled President François Hollande to increase defense spending; in 2016, defense expenditures rose by $671 million, bringing total defense spending to $32 billion.[378] While this amount is still several billion less than the 2015 figure, it shows that France may be headed in a more security-driven direction. In 2016, approximately $19 billion was allocated toward equipment procurement, including nine *Rafale* multirole fighters, eleven combat and transport helicopters, 25 heavy vehicles, one missile-outfitted frigate, and one Barracuda attack submarine.[379] In 2016, the French were also expected to spend $4 billion on research and development (R&D) and an undisclosed amount on cyber warfare and intelligence.[380] Because of these spending trends, if NATO were to respond to cyber aggression with military force, it is likely that France would be able to fiscally support a significant role in these operations.

376 "Defense Expenditures of NATO Countries," 6.

377 Ashley Kirk, "European Debt Crisis: It's Not just Greece that's Drowning in Debt," *The Telegraph*, June 29, 2015, http://www.telegraph.co.uk/news/worldnews/europe/greece/11705720/European-debt-crisis-Its-not-just-Greece-thats-drowning-in-debt.html, 1.

378 Ryan Maass, "France to Increase Defense Spending in 2016," United Press International, October 2, 2015, http://www.upi.com/Business_News/Security-Industry/2015/10/02/France-to-increase-defense-spending-in-2016/4561443814370/, 2.

379 Maass, "France to Increase Defense Spending," 2.

380 Maass, "France to Increase Defense Spending," 2; Kumaran Ira, "France Boosts Military Spending, Recruits More Youth into the Army," May 23, 2015, https://www.wsws.org/en/articles/2015/05/23/fran-m23.html, 1; *French White Paper*, Presidency of the French Republic, 100.

2. Germany

As the fourth largest economy in the world and the largest economy in Europe, Germany spends about 1.18 percent of its GDP on defense.[381] During the period of European austerity (2010-2015),[382] Germany's defense spending as a percentage of GDP declined by 13 percent.[383] Like France, Germany does not meet NATO's 2 percent of GDP recommendation, but it still spends in real terms more on defense than 90 percent of the governments in the rest of the world.[384] Additionally, out of the five NATO nations assessed in this thesis, Germany has the least national debt in relation to GDP. 2016 economic figures hold Germany's debt to GDP at just under 75 percent.[385]

Due to regional security concerns deriving from the emergence of violent extremism and a resurgent Russia, Germany recently pledged to raise its defense spending gradually to 2 percent of GDP.[386] In fact, in early 2016, German Chancellor Angela Merkel approved a defense budget increase of 2.7 percent to address the country's worsening refugee problem.[387] Yet, according to experts from the German defense ministry, the €36.6 billion (about $40 billion) defense plan will be insufficient to keep the German Armed Forces functional and will not fund necessary investments in military equipment.[388] It remains to be seen whether the upsurge of terrorist attacks—like the ones that took place across Germany in May and July 2016—will have any effect on Chancellor Merkel's defense spending calculus. For now, due to poor budgetary

---

381 "Defense Expenditures of NATO Countries," 6, 7; Bajpai, "World's Top Economies," 2.

382 Jennifer Pietras, "Austerity Measures in the EU—A Country by Country Table," *European Affairs*, accessed August 3, 2016, http://www.europeaninstitute.org/index.php/112-european-affairs/special-g-20-issue-on-financial-reform/1180-austerity-measures-in-the-eu, 1–3.

383 "Defense Expenditures of NATO Countries," 8.

384 "Defense Budget by Country," 1.

385 Kirk, "European Debt Crisis," 1.

386 Michael Rühle, "Security Policy as Symbolism," *Berlin Policy Journal*, February 2016. http://berlinpolicyjournal.com/security-policy-as-symbolism/, 3.

387 Birgit Jennen and Rainer Buergin, "Merkel Seeks Security Spending Boost in Budget Driven by Crises," Bloomberg, March 22, 2016, http://www.bloomberg.com/news/articles/2016-03-22/merkel-seeks-defense-boost-in-german-budget-driven-by-crises, 1.

388 "Debate over German Defense Budget Surfaces," Bundeswehr, May 21, 2016, http://www.dw.com/en/debate-over-german-defense-budget-surfaces/a-19275360, 1.

prospects for the German Armed Forces, it is unlikely that Germany would be able to fiscally sustain a significant role in coalition operations if NATO responded to cyber aggression with military force.

3. Italy

Italy has the eighth largest economy in the world and the fourth largest economy in Europe.[389] Out of the top five NATO members, it spends the least on defense both in relative and absolute terms. In 2016, it allocated only about 0.95 percent of GDP toward defense spending, which equates to approximately $18 billion.[390] Additionally, Italy maintains one of the world's highest government deficits in relation to GDP; at a staggering 132 percent, Italy is right behind Greece in terms of relative debt ratio in Europe.[391] It remains to be seen whether Italy will require a European financial bailout.

With a youth jobless rate approaching 40 percent and an economy that has barely grown since 1999, Italian Prime Minister Matteo Renzi has instituted various reforms to address some of the nation's most pressing economic and political challenges.[392] While Renzi has led initiatives designed to reduce some of the fiscal waste in his country, Italy's polity and powerful labor unions have limited progress. Italy struggles with bureaucratic gridlock, economic stasis, poor bank-lending laws, tax evasion, labor issues, and inefficiencies in its public administration.[393] In comparison to these national problems, Italy's cyber issues take a backseat. Although Renzi approved a $165 million investment in cybersecurity in the wake of the 2015 Paris attacks,[394] this will do little to improve the problems associated with Italy's current fledgling digital infrastructure.

---

389 Bajpai, "World's Top Economies," 3; "Defense Expenditures of NATO Countries," 8.

390 "Defense Expenditures of NATO Countries," 6.

391 Kirk, "European Debt Crisis," 1.

392 Tony Barber, "Renzi is the Last Hope for the Italian Elite," *Financial Times*, January 2, 2015, http://www.ft.com/intl/cms/s/0/21f3bf46-86cd-11e4-9c2d-00144feabdc0.html#axzz43Q9c9qW9, 1–2; Andrew Walker, "What's the Problem with Italian Banks?," *BBC News*, July 10, 2016, http://www.bbc.com/news/business-36708357, 1.

393 Barber, "Renzi is the Last Hope," 1–2; Walker, "What's the Problem with Italian Banks?," 1.

394 Thomas D. Williams, "Prime Minister Announces One Billion Euros for Security," November 24, 2015, http://www.breitbart.com/national-security/2015/11/24/italian-prime-minister-announces-adding-1-billion-euros-for-security/, 1.

Having just bailed out Italy's third-largest bank—*Monte dei Paschi di Siena*—during the country's worst banking crisis, Renzi awaits the results of a referendum on constitutional reform, which—like in the UK—will determine the future of his government.[395] The referendum, currently scheduled for November 2016,[396] is designed to minimize the political gridlock plaguing Italy's government by making the following changes: reducing the Senate from 315 to 100 seats, selecting Senators based on regional appointments instead of direct elections, and limiting the legislative powers of the Senate.[397] While Italians desire change, increasing frustration over immigration and economic issues may factor heavily into Italian voters' political decisions in November.[398] With the prospect of an EU bailout and the potential for Italians to usher in new national elections (depending on the results of the referendum),[399] the likelihood of an increase in Italian defense spending within the near future is low. If NATO were to respond to cyber aggression with military force, it is doubtful whether Italy could fulfill or fiscally sustain any significant role in these operations.

4. United Kingdom

The UK is one of the five NATO members that spends the recommended 2 percent or more of GDP on national defense. Yet its debt is also 89 percent of GDP.[400] With the UK having voted in the June 2016 referendum to exit the EU, the country's economic future is uncertain. Since the referendum, economic data has shown that

395 "Renzi Should Make a Hard Push for Stimulus," *Financial Times*, August 14, 2016, http://www.ft.com/cms/s/0/bb4f7be8-607f-11e6-b38c-7b39cbb1138a.html#axzz4HNax3eK4, 1.

396 Stephanie Kirchgaessner, "Will Italy be Europe's Next Casualty as Renzi Risks All on Referendum?," *The Guardian*, August 6, 2016. https://www.theguardian.com/world/2016/aug/06/matteo-renzi-italy-referendum-banks-brexit, 1.

397 Chiara Albanese and John Follain, "A Prime Minister, a Referendum, and Italy's Turn to Get Worried," Bloomberg, July 4, 2016, http://www.bloomberg.com/news/articles/2016-07-04/a-prime-minister-a-referendum-and-italy-s-turn-to-get-worried, 2; James Newell, "Italy's Looming Referendum is Giving PM Matteo Renzi Sleepless Nights," August 15, 2016, http://theconversation.com/italys-looming-referendum-is-giving-pm-matteo-renzi-sleepless-nights-63844, 1.

398 Kirchgaessner, "Will Italy be Europe's Next Casualty?," 2.

399 Kirchgaessner, "Will Italy be Europe's Next Casualty?," 2.

400 Kirk, "European Debt Crisis," 1.

inflation has skyrocketed in the UK.[401] In addition, the British Pound Sterling (GBP) reached one of its lowest values in the last decade, falling precipitously in the aftermath of the vote (nearly 10 percent); the GBP also declined about 16 percent during the last year (from August 2015 to August 2016).[402] Currently, the GBP is trading at 1.29 GBP to the U.S. dollar (USD).[403] The "Brexit" decision will have macroeconomic outcomes on the country's free trade, foreign direct investment, and immigration.[404] (It will also have consequences for the UK's—and possibly America's—strategic influence in Europe.)

As the fifth largest economy in the world and the second largest economy in Europe—after Germany—the UK spends about $55 billion annually on defense, making it one of the world's highest national spenders on defense and security.[405] The UK also has a history of sound investment in information technology and cybersecurity. In 2015, the UK increased its cyber budget by 76 percent to £1.9 billion (about $2.85 billion, based on 2015 currency exchange rates), or half of the U.S. cyber budget.[406] As part of this budgetary increase, Parliament approved the establishment of two cyber innovation centers and a Defense and Cyber Innovation Fund to encourage the development of advanced digital capabilities.[407] Due to consistent British investments in cyber technology and strong defense expenditure prospects, it is likely that the UK would be able to fiscally support coalition operations if NATO responded to cyber aggression with military force.

---

401 Yoel Minkoff, "U.K. Inflation Gets Post-Brexit Boost," Seeking Alpha, August 16, 2016, http://seekingalpha.com/news/3203602-u-k-inflation-gets-post-brexit-boost?ifp=0&source=email_wsb&utoken=3c2dc8ae2e2c23ed12620e168ca55b40, 1.

402 "British Pound," Trading Economics, accessed August 16, 2016, http://www.tradingeconomics.com/united-kingdom/currency, 1.

403 "British Pound," 1.

404 Kristin Archick, *The European Union: Current Challenges and Future Prospects* (CRS Report No. R44249), Washington, DC: Congressional Research Service, 2016, https://www.fas.org/sgp/crs/row/R44249.pdf, 1, 15.

405 "Defense Budget by Country," 1; Bajpai, "World's Top Economies," 2.

406 "Spending Review: Chancellor Confirms £1.9bn Cybersecurity Funding," IT Pro, November 25, 2015, http://www.itpro.co.uk/security/25657/spending-review-chancellor-confirms-19bn-cybersecurity-funding, 1–2.

407 "Spending Review," 2.

5. United States

The United States is the global leader in both economic and defense spending terms. With a $19 trillion GDP, the United States contributes over a half a trillion dollars to defense requirements or about 3.62 percent of GDP.[408] While U.S. defense expenditures represent about 72 percent of NATO's total military expenditures,[409] the United States directly contributes about 22 percent of NATO's common funding.[410] Nonetheless, per Figure 1, the United States has reduced its defense spending by 28 percent since 2008.[411] This reduction in spending may be correlated to troop drawdown numbers in the Middle East and to the amount of debt the United States has incurred over the last decade. America's debt represents over 100 percent of its economic output, making it one of the most indebted nations in the world. However, the United States spends the most by far on cyber defense. Between 2016 and 2020, U.S. cyber spending, including on science and technology, information assurance, and cyberspace operations, will aggregate to $27 billion—or about $5.4 billion each year.[412] Consistent cyber investments have enabled the United States to maintain its position at the forefront of global digital competition. Despite its large deficit, the United States' prominent investments in defense and cybernetic capabilities would likely enable it to fiscally support coalition operations if NATO responded to an act of cyberwar with military force.

Out of the five primary military spenders in the Alliance, only two meet NATO's recommended 2 percent spending guideline: the UK and the United States. Budget cuts have proven to be the chief factors behind steady declines in Western military readiness,

---

408 Bajpai, "World's Top Economies," 1; "Defense Expenditures of NATO Countries," 6.

409 "Defense Expenditures of NATO Countries," 6.

410 Jon Greenberg, "Sanders Oversimplifies U.S. Share of NATO," April 19, 2016, http://www.politifact.com/truth-o-meter/statements/2016/apr/19/bernie-s/sanders-oversimplifies-us-share-NATO/, 3.

411 "Defense Expenditures of NATO Countries," 6.

412 Aliya Sternstein, "The Military's Cybersecurity Budget in 4 Charts," *Defense One*, March 16, 2015, http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/, 1–2.

with personnel and equipment shortfalls serving as the first consequences of this trend.[413] Yet what have been the reasons for the reductions in defense spending? Several variables have affected and limited the Allies' military spending over the years, including the global financial crisis, European austerity measures, growing demands on European social welfare programs, and complacent and naïve assumptions about security requirements.[414] While a prosperous and secure Europe strategically benefits the United States, America's continued financing of European security has been a chief concern for NATO and the United States for decades. A poor showing of defense spending by top European Allies and an overreliance on the American security apparatus could strategically undermine NATO's valued deterrent capability. If the majority of the Allies fail to prioritize their own security and opt to "free ride" on a capable few, what does this say about NATO's solidarity, resolve, and capability? Moreover, if spending trends serve as an important indicator of national priorities and political will, then declining defense budgets paint a bleak picture for NATO's commitment to common defense.[415]

Despite downward spending trends, most Allied governments recognize the pervasive need to reinforce their cybernetic critical infrastructures. Over the last decade, NATO's policies on cyber defense have progressively evolved to bring cybersecurity matters to the forefront of Alliance defense and resource allocation efforts.[416] In fact, most of the Alliance's leading members, namely France, Germany, the UK, and the United States, prioritize cyber defense highly within their defense budgets. Nonetheless, the cybersecurity prioritization of NATO members should not be taken in a vacuum; it must be balanced against overall defense spending trends. On one hand, many top Allied states have increased their cybersecurity investments and public affirmations of their commitment to meeting NATO's 2 percent spending guideline; yet on the other, sharp declines in defense spending tell a different story. If NATO were compelled to respond to

413 Shea, "Keeping NATO Relevant," 3.

414 Iain Begg, Fabian Mushovel, and Robin Niblett, "The Welfare State in Europe: Visions for Reform," Chatham House, September 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150917WelfareStateEuropeNiblettBeggMushovel.pdf, 4.

415 "Funding NATO," 1.

416 "Cyber Defense Pledge," NATO, July 8, 2016, http://www.nato.int/cps/en/natohq/official_texts_133177.htm, 1.

cyber aggression with armed force, the ability of some Alliance members to finance a significant role in these operations would be in serious question. Thus, disparate cyber and defense spending trends have moderately prepared NATO to effectively resolve cyber aggression with cybernetic measures and military force. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 2 in defense spending.

G. DEFENSE POLICY PRIORITIZATION

The purpose of this section is to evaluate the defense policy priorities and readiness of top NATO Allies to respond effectively to major acts of cyberwar using military measures. Only the defense policies of the Alliance's leading members—France, Germany, Italy, the UK, and the United States—have been assessed because of the level of political and military weight they bring to bear within NATO.

1. France

France has one of the most active defense policies in Europe and, likewise, one of the most forward-deployed armed forces in the world.[417] French defense policy is based on an operational model that differentiates its force requirements by mission set.[418] The armed forces must be coordinated, adaptable, and combat ready to operate in dynamic threat environments to support deterrence, crisis management, protection, and clandestine operations.[419] A key component and priority of French military strategy is international intervention, which France views as essential to not only safeguarding its own sovereignty and national interests but also to supporting global peace and security.[420] While France will consistently seek coalition support and legitimacy in action through the endorsement of international institutions, notably the United Nations (UN) and/or the European Union (EU), history has proven that it is not afraid to act unilaterally.[421]

---

417 Jeremy Bender, "France's Military is All Over Africa," January 22, 2015, *Business Insider*, http://www.businessinsider.com/frances-military-is-all-over-africa-2015-1, 1.

418 *White Paper: Defense and National Security: Twelve Key Points*, Presidency of the French Republic, 2013, http://www.rpfrance-otan.org/White-Paper-on-defence-and, 5.

419 *French White Paper*, Presidency of the French Republic, 80–81.

420 *French White Paper*, Presidency of the French Republic, 80.

421 *French White Paper*, Presidency of the French Republic, 74, 80, 89, 117.

France's policy of intervention is evidenced in its numerous overseas bases and operations in Africa and the Middle East.[422] The French maintain four permanent bases in Djibouti, Gabon, Senegal, and the French territory of La Réunion in the Indian Ocean.[423] The primary purpose of France's military presence in Djibouti, Gabon, and Senegal is to promote French influence and regional stability and security.[424] France operates out of La Réunion in order to quickly deploy forces and coordinate support and contingency operations, particularly in the Central African Republic (CAR), Chad, Côte d'Ivoire, Mali, and Somalia.[425]

Since 1964, France has led more than 50 military interventions in Africa, which have ranged in scope from humanitarian, peacekeeping, and non-combatant evacuation operations (NEO) to counterinsurgency, combat support, and security missions.[426] The French have led stability operations to varying degrees in the CAR since 2008, in Côte d'Ivoire since 2002, and in Chad since 1986 to combat rising jihadism and sectarian violence.[427] One of the French military's most recent interventions was Operation Serval in Mali—a two-year counterinsurgency campaign that successfully drove Al-Qaeda militants out of the country.[428] In total, France has approximately 6,500 troops deployed in out-of-area (OOA) operations across Africa.[429] France's history of intervention has yielded certain advantages. For example, the French military enjoys strategic access and

---

422 Ryan McMaken, "Hey Big Spender: France's Robust Military Spending," Mises Wire, November 17, 2015, https://mises.org/blog/hey-big-spender-frances-robust-military-spending, 7.

423 "France's Military Ties with Africa Strengthen," The Economist Intelligence Unit, May 21, 2014, http://country.eiu.com/article.aspx?articleid=1801832364&Country=Chad&topic=Politics, 1.

424 John C. K. Daly, "Counterterrorism or Neocolonialism? The French Army in Africa," *Terrorism Monitor,* 12, no. 5 (2014), http://www.jamestown.org/regions/africa/single/?tx_ttnews%5Btt_news%5D=42051&tx_ttnews%5BbackPid%5D=55&cHash=8e372fe5ecd8a63b4cfccecb1544d46e#.V7AtE5grK01, 2.

425 "France's Military Ties with Africa Strengthen," 1; Daly, "Counterterrorism or Neocolonialism?," 3.

426 *50 Years of Operations in Africa (1964-2014), Defense Ministry of the French Republic, Cahier du RETEX—Research,* April 2016, http://www.cdef.terre.defense.gouv.fr/content/download/5870/75552/file/20160606_50-ans-d-OPEX-Afrique_US.pdf, 15–17.

427 Bender, "France's Military is All Over Africa," 4–6.

428 Bender, "France's Military is All Over Africa," 3.

429 *50 Years of Operations in* Africa, 20, 23.

freedom of movement across much of Africa, including Burkina Faso, Chad, Mali, Mauritania, and Niger.[430]

Following the November 2015 Paris attacks, President Hollande approved defense measures that would increase the number of troops stationed in France from 7,000 to 10,000.[431] However, France has also cut its military significantly in the past decade. In fact, out of the 28 Allies, France incurred the largest proportional drop in military personnel numbers between 2008 and 2015—approximately 41 percent; military personnel today total around 207,000.[432] Yet, as previously discussed, these declining numbers have not diminished France's strategic footprint abroad.

In addition to projecting a global forward presence, French defense policy recognizes that France must support national investments in science, technology, and specifically cyber defense.[433] In fact, the body of the *French White Paper* explicitly mentions the term "cyber" 40 times; it further dedicates two pages to delineating how the government will strengthen its cyber defenses, such as through clearly defined security protocols, close cooperation with private and state agencies, and through the modernization of existing information technology suites.[434] The defense policy even outlines a possible scenario in which a major act of cyber aggression could escalate into armed aggression and war.[435] The French government has been subject to countless cyber attacks over the years, so its concern about macro-level cybernetic aggression aimed at its national information infrastructure is understandable.[436] The French government views cyber attacks as potential strategic threats to sovereignty, security, and national repute.[437] For these reasons, the French have developed both offensive and defensive cybernetic

430 Bender, "France's Military is All Over Africa," 2.

431 Peter B. de Selding, "Paris Attacks Pressure French Defense Budget as New Space Programs Ramp Up," *SpaceNews*, November 19, 2015, http://spacenews.com/paris-attacks-pressure-french-defense-budget-as-new-space-programs-ramp-up/, 1.

432 "Defense Expenditures of NATO Countries," 8.

433 *French White Paper*, Presidency of the French Republic, 20.

434 *French White Paper*, Presidency of the French Republic, 100–102.

435 *French White Paper*, Presidency of the French Republic, 48.

436 *French White Paper*, Presidency of the French Republic, 43.

437 *French White Paper*, Presidency of the French Republic, 48, 100.

capabilities.[438] In 2015, the government published its newest, most robust cyber strategy, which underscored the high threat prioritization level that cybersecurity has assumed in French defense culture.[439]

2. Germany

Some security experts perceive Germany's foreign and defense policies as a model of commercial realism—meaning that its policies are geo-economically motivated in their approach to politico-military matters.[440] For Germany, these experts contend that economic considerations can undermine the employment of military force when certain geopolitical state actors, like Russia, are involved.[441] While many factors influence Berlin's political decision making, some policy experts and senior German officials assert that Germany is on its way to increasing its defense commitments and role in security affairs.[442]

Yet, Germany's past policy decisions have given it a reputation for being a security free-rider. Since 2008, the size of Germany's armed forces has been reduced by 28 percent, with current numbers totaling approximately 180,000.[443] According to Claudia Major and Christian Molling—two prominent German scholars—Germany's nonparticipation in various UN and EU operations like Chad in 2008 and Côte d'Ivoire in 2011 illustrated a lack of will on the part of an able Ally to take on international responsibilities commensurate with its power.[444] When Berlin does choose to get involved in global security engagement, it typically does so under the auspices of the UN,

---

438 *French White Paper*, Presidency of the French Republic, 89.

439 *French National Digital Security Strategy*, Defense Ministry of the French Republic, October 19, 2015, http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf, 8, 33.

440 Stephen F. Szabo, "Germany's Commercial Realism and the Russia Problem," *Survival: Global Politics and Strategy* 56:5 (2014): 117–128, doi: 10.1080/00396338.2014.962799, 119.

441 Szabo, "Germany's Commercial Realism," 123, 125.

442 Claudia Major and Christian Molling, *German Defense Policy in 2014 and Beyond: Options for Change.* Notes du Cerfa, 113, Paris: Study Committee for Franco-German Relations, June 2014, https://www.ifri.org/sites/default/files/atoms/files/ifri_noteducerfa113majorandmollingeng.pdf, 5.

443 "Defense Expenditures of NATO Countries," 8.

444 Major and Molling, *German Defense Policy in 2014 and Beyond*, 7.

EU, or NATO.[445] Yet if Germany chooses to reformulate its defense strategies, it might begin by obtaining public support and improving the nation's overall perception of the armed forces.[446] While the German government would unquestionably honor its Article 5 commitments if an act of aggression threatened a member state, Germany would prefer for NATO to focus more on collective defense and less on crisis management operations, like Kosovo in 1999 and Libya in 2011.[447]

The government's cautious policies and geo-economic priorities have strategic implications concerning Germany's willingness to involve itself in future armed conflicts that could originate in cyberspace. It is likely that, rather than taking the lead in operations in a cybernetic conflict, Germany would assume a supporting role in a NATO-led operation; the nature of its contribution would probably resemble past logistical support as shown (for example) in its EU mission in the CAR.[448]

While Germany's *White Paper 2006* focused on the threats of international terrorism, weapons proliferation, and destabilization resulting from regional conflicts, its defense policy has undergone considerable revision.[449] In July 2016, Germany released the *White Paper 2016.* In contrast to the 2006 defense document, which referenced cyber only once in passing, the 2016 paper discussed cyber a notable 76 times.[450] While both defense policies identified transnational terrorism, global arms proliferation, and instability from fragile states as chief security concerns, *White Paper 2016* addressed the emergence of three additional challenges: hybrid warfare, cyber attacks, and migration.[451]

---

445 Major and Molling, *German Defense Policy in 2014 and Beyond*, 12, 14.

446 Major and Molling, *German Defense Policy in 2014 and Beyond*, 8.

447 Major and Molling, *German Defense Policy in 2014 and Beyond*, 12.

448 Major and Molling, *German Defense Policy in 2014 and Beyond*, 14.

449 *White Paper 2006: On German Security Policy and the Future of the Bundeswehr*, Federal Ministry of Defense, 2006, http://responsibilitytoprotect.org/Germany_White_Paper_2006.pdf, 6, 14, 18.

450 *White Paper 2016: On German Security Policy and the Future of the Bundeswehr*, Federal Ministry of Defense, 2016, https://cle.nps.edu/access/content/group/cebb1f88-2b49-4223-8047-b53ee880fc91/Germany-White-Paper-2016.pdf.

451 *White Paper 2016*, Federal Ministry of Defense, 8, 28.

The German government has had a strong cybersecurity policy and legal framework in place since 2011 and a national critical infrastructure protection strategy since 2009.[452] In addition, Germany's cyber defense policies are strategically aligned with NATO's cyber strategy. Like NATO, the German government has acknowledged the increasing challenges that cyber attacks present, including the difficulties with attribution and deterrence and the limitations of international laws and confidence-building measures.[453] According to the *White Paper 2016*, "The effects of cyber attacks can equal those of armed conflicts and may escalate into the non-virtual world." For both NATO and Germany, cyber events that cross this threshold could pull the conflict into the kinetic domain.[454]

3. Italy

Like many European Allies, Italy views NATO membership not only as a strategic linkage to the United States and Europe, but also as a critical means of sharing the economic burdens associated with national defense.[455] Between 2008 and 2015, the Italian military decreased its force strength by 7 percent; today the Italian armed forces consist of roughly 182,000 personnel.[456]

Italy's 2015 *White Paper for International Security and Defense* identifies four key objectives for its armed forces: (1) national defense, (2) defense of the Euro-Atlantic and Mediterranean regions, (3) contributions to international operations for peace, security, and stability, and (4) contributions to joint operations and tasks.[457] Recognizing its governance shortfalls in management, communication, and integration, Italy's defense policy calls for additional governmental transparency and improved interagency

---

452 "Country: Germany," BSA, accessed March 19, 2016, http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf, 1.

453 *White Paper 2016*, Federal Ministry of Defense, 36–37.

454 *White Paper 2016*, Federal Ministry of Defense, 37.

455 *White Paper for International Security and* Defense, Ministry of Defense of the Republic of Italy, 2015, http://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf, 6.

456 "Defense Expenditures of NATO Countries," 8.

457 *White Paper*, Ministry of Defense of the Republic of Italy, 18–19.

cooperation.[458] While the Italian government does not share France's level of support for foreign intervention, Italy does view itself as a global actor willing to engage in coalition missions with the international backing of the UN, the EU, or NATO.[459] Because Italy's economic and defense priorities strongly align with the rest of the EU, the Italians—along with the French—consistently pursue increased European integration and cooperation within the economic, political, and military spheres of governance.[460]

As for cyber defense, Italy's defense policy succeeds in highlighting the increased significance of the cybernetic domain but only references cyber eight times in the 2015 white paper. Italy's published national security policy fails to articulate concrete plans for the development of digital capabilities in cyber innovation, deployment, and defense.[461] However, the Italian government has attempted to make up for its lack of cyber threat prioritization with the formulation of its national cyber strategy, the 2013 *National Strategic Framework for Cyberspace Security*.[462]

4. United Kingdom

The UK's 2015 *Strategic Defense and Security Review* (SDSR) was issued in a geopolitical and budgetary context vastly different from its 2010 SDSR release.[463] In the 2010 review, the government made significant cuts to the armed forces and equipment. In fact, the government reduced the UK's military force by 16 percent between 2008 and 2015 to a total of 162,000 personnel.[464] By 2015, much had changed; the British economy had recovered from the global financial crisis, and the UK's NATO defense commitments in Afghanistan with the International Security Assistance Force (ISAF) had

458 *White Paper*, Ministry of Defense of the Republic of Italy, 5.

459 *White Paper*, Ministry of Defense of the Republic of Italy, 13.

460 *White Paper*, Ministry of Defense of the Republic of Italy, 14–15.

461 *White Paper*, Ministry of Defense of the Republic of Italy, 9.

462 *Italy's National Strategic Framework for Cyberspace Security*, Presidency of the Council of Ministers, 2013, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf.

463 Louisa Brooke-Holland, "The 2015 SDSR: A Primer," House of Commons, November 19, 2015, http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7235, 2.

464 "Defense Expenditures of NATO Countries," 8.

concluded.[465] Russia and ISIL had emerged as the new threats *du jour*, and global instability and ethno-sectarian violence in North Africa and the Middle East had generated a refugee crisis threatening European solidarity. Given the aforementioned global challenges, in 2015 the British government recommitted to restructuring and re-investing in the military to render it better prepared and equipped to safeguard national security interests.[466]

The 2015 SDSR set the UK back on the right track and properly examined the requirements for increasing the size and readiness of the UK's naval fleet and expeditionary forces.[467] According to the SDSR, the UK plans to develop a highly agile Joint Force 2025, which will include a maritime and special forces task group, a new land division strike force, and two new Queen Elizabeth Class aircraft carriers.[468] While the defense policy underscores the need for the UK to expand its global reach, enhance its power projection, and increase its material and strategic investments in NATO, one of the UK's top three national priorities is to remain a strategic vanguard in the area of cyber defense.[469]

Like NATO, the UK recognizes that foreign cyber aggression against critical infrastructure is a major economic and security threat.[470] According to the SDSR, the government will treat any form of asymmetric damage caused by cyber attacks as seriously as an "equivalent conventional attack."[471] The British government not only references cyber an impressive 109 times in the SDSR, it also has an entire section dedicated to cyber defense and a progressive national cyber strategy published in

---

465 Brooke-Holland, "The 2015 SDSR: A Primer," 2.

466 *National Security Strategy and Strategic Defense Security Review: A Secure and Prosperous United Kingdom*, Her Majesty's Government, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf, 6.

467 *National Security Strategy*, Her Majesty's Government, 6.

468 *National Security Strategy*, Her Majesty's Government, 29.

469 *National Security Strategy*, Her Majesty's Government, 9–10.

470 *National Security Strategy*, Her Majesty's Government, 18.

471 *National Security Strategy*, Her Majesty's Government, 19.

2011.[472] The UK—along with France, Germany, and the United States—employs the "full spectrum" of capabilities, which includes an offensive cyber policy for defense.[473] With the establishment of cutting-edge cyber assessment, intelligence, and response centers across the country and a focus on strengthening cyber innovation domestically, the UK pursues an active approach to defense.[474]

5. United States

The U.S. military is regarded as the largest, most advanced, and most combat ready military on the planet, able to execute multiple mission sets across all warfare domains. Of the five NATO Allies discussed, U.S. military force strength has been reduced the least since 2008—about 6 percent.[475] Today, America's armed forces total 1.3 million.[476] With military bases present in more countries than any other nation-state, the United States has the largest global strategic footprint of any national power.

While the *National Military Strategy* lists revisionist state adversaries like Russia and violent extremist organizations like ISIL as top threats to American security, cyber defense remains a high priority for the U.S. Defense Department.[477] In 2013, National Intelligence Director James Clapper affirmed that cyber aggression represented "new and unpredictable" threats to American security, asserting that foreign intelligence services had succeeded in compromising countless government and corporate systems in the unclassified and classified domains.[478] According to the 2016 Worldwide Threat Assessment of the U.S. Intelligence Community, U.S. critical infrastructure and supply

---

472 *National Security Strategy*, Her Majesty's Government, 40.

473 *National Security Strategy*, Her Majesty's Government, 24, 41.

474 *National Security Strategy*, Her Majesty's Government, 40–41.

475 "Defense Expenditures of NATO Countries," 8.

476 "Defense Expenditures of NATO Countries," 8.

477 *The National Military Strategy of the United States of America*, U.S. Joint Chiefs of Staff, Washington, DC, 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf, 5, 11.

478 James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Select Committee on Intelligence: Washington, D.C., 2013, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-090.pdf, 1–2.

chain networks, especially in the healthcare sector, remain vulnerable to cyber attack.[479] The updated threat assessment specifically listed China, Iran, North Korea, and Russia as the principal cyber threats to the United States.[480]

As shown, the defense polices of NATO's five leading member states are similar in their strategic focus but disparate in scope and character. France, the UK, and the United States maintain the most active defense strategies, profiting from global basing and strategic access and leading frequent expeditionary missions and training exercises. These state actors prefer to have political support from international institutions but are unafraid to act both unilaterally and preemptively if doing so serves their national interests. Germany and Italy are staunch advocates for European solidarity and thus subscribe (to a greater extent than France, the UK, and the United States) to a liberal international model of cooperation and consensus. Germany's and Italy's reticence to intervene in some international crises stems from their history and their reliance and trust in international institutions such as the United Nations, NATO, and the European Union.

Cybernetically, the digital postures and policies in these Allied nations reveal an active strategic outlook. While the United States invests significantly more on cyber readiness than its Allies, the UK and France nonetheless prioritize cyber defense highly in their defense budgets. Over the past few years, Germany has made considerable progress in strengthening the digital defenses of its critical infrastructure. Out of the top most influential Allies in NATO, Italy has the furthest to go with its cybernetic efforts and must gradually allocate more resources and programs toward cybersecurity.

If the Alliance responded to a major act of cyberwar, France, the UK, and the United States would probably be in the best positions to lend their cybernetic capabilities to the Ally in need. The active security policies of France, the UK, and the United States also may make them more likely to approve a NAC decision for a response of force to a cyber attack that reaches the threshold of an armed attack. Conversely, the more

479 James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Armed Services Committee: Washington, D.C., 2016, https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf, 2.

480 Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," 2016, 3.

restrained defense policies of Germany and Italy may make them less likely to support military intervention in the same regard. Thus, the national security plans, defense objectives, and threat priorities of the top five Allied member states have moderately prepared NATO to effectively address cyberwar aggression through both cybernetic means and military force. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 2 in defense policy prioritization.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

After evaluating the measures of effectiveness of NATO's cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization, this thesis assesses that NATO is moderately prepared to respond effectively to a major act of cyberwar against one or more of the Allies. While the Alliance is well prepared to address major acts of cyberwar in the cyber dimension, it is less prepared to respond to the same threats with military force.

NATO scored the highest in the areas of cyber strategy and cyber cooperation, meeting or exceeding most standards of readiness to effectively address, counter, and/or resolve a major act of cyberwar launched against one or more of its members. The Alliance scored moderately in the areas of decision making, defense spending, and defense policy prioritization, meeting the minimum standards of readiness to effectively address, counter, and/or resolve a major act of cyberwar launched against one or more of the Allies. Finally, NATO scored the lowest in the areas of political will and crisis management, failing to meet minimum standards of readiness to effectively address, counter, and/or resolve a major act of cyber aggression against one or more of its members. Table 1 provides a summary of how prepared NATO is across the seven key areas examined in this study:

Table 1. NATO's Level of Preparedness for Cyberwar

Areas of Analysis	**Numerical Ranking**	**Qualitative Ranking**
Cyber Strategy	3	High
Cyber Cooperation	3	High
Decision Making	2	Moderate
Political Will	1	Minimal
Crisis Management	1	Minimal
Defense Spending	2	Moderate
Defense Policy Prioritization	2	Moderate
Overall Score	**2**	**Moderate**

Note: Scores range from 1–3, with 1 being the lowest and 3 being the highest level of preparedness.

A. RECOMMENDATIONS

Although NATO has made significant policy and structural changes to its organization in order to address cybernetic challenges, it still faces institutional, political, economic, and decision-making hurdles. After analyzing the level of preparedness of NATO's cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization, some shortfalls and challenges therein were identified; this thesis recommends the following improvements in policy and effort:

1. Cyber Strategy

The Alliance has made substantial enhancements to its policies for addressing cybernetic incidents and attacks. NATO's organizational evolution against a backdrop of cyber aggression has yielded transformations in cyber policy and given rise to the establishment of sophisticated cyber defense agencies that enable the Alliance to respond capably to cybernetic threats. The institutional and structural changes that the Alliance has made have shown how sensitive and responsive it has been to cyber attacks happening within its European periphery.

NATO's robust Cyber Defense Policy has facilitated the establishment of several advanced cyber entities, including the Cyber Defense Management Authority (CDMA), the NATO Communications and Information Organization (NCIO), the NATO Communications and Information Agency (NCIA), the NATO Computer Incident Response Capability (NCIRC), the Communications and Information Systems (CIS) Group, and the Rapid Reaction Teams (RRTs). Through its state-of-the-art information technology (IT) resources and cyber agencies, NATO maintains an advanced level of cyber monitoring, technical and legal management, and resolution capability. The Alliance's deliberate policy of ambiguity regarding the parameters that would constitute an armed attack affords it a significant strategic advantage. In all, the organization's progressive cyber strategy has effected a marked improvement in its cyber defense posture, which has highly prepared NATO to cybernetically address,

counter, and resolve major acts of cyber aggression against one or more of its members in cyberspace.

Despite these cyber achievements, however, there is room for improvement. NATO's official cyber mission is defensive in nature; indeed, the NCIA and NCIRC focus purely on cyber defensive strategies and measures.[481] Yet, there is a critical need for the Alliance to develop an offensive cyberwarfare strategy to supplement its cyber defense program. China and Russia along with roughly 30 countries have cyber offensive policies.[482] To get ahead of these security challenges, the Alliance must develop its own organic cyber offensive capability. Since NATO values its official position as a military defense Alliance, there are steps that it could take to that end.

The Alliance could establish a new center—namely a NATO Hybrid Warfare Center of Excellence—specifically mandated to analyze emerging security threats and crises and actively train for and counter these hybrid threats through asymmetric means, including through cyber counter-offensive operations launched against enemy networks. The center could consist of a cyber offensive element whose primary objectives would be to rehearse kinetic cyber operations, deepen NATO's understanding of enemy cyber capabilities and activities, and deliver offensive cyber effects on the information systems of its adversaries as needed. Because the centers of excellence are not part of NATO's official command structure, are not directly funded by NATO, and follow a different set of rules,[483] NATO does not officially or automatically endorse their products or activities. NATO would have the option to accept, share in, or reject the center's cyber policies, actions, recommendations, and intelligence products on a case-by-case basis. A Hybrid Warfare Center of Excellence could further help address NATO's planning, response, and intelligence shortfalls, which it experienced during the Russian-sponsored hybrid and cyberwarfare campaigns

481 Morbin, "NATO: Defending Against the Known Unknowns," 1–2.

482 Klimburg, *National Cybersecurity Framework Manual*, 17.

483 Klimburg, *National Cybersecurity Framework Manual*, iv; Guy B. Roberts, "NATO'S Centers of Excellence: A Key Enabler in Transforming NATO to Address 21st Century Security Challenges," *Working Paper*, October 8, 2014, http://www.stanleyfoundation.org/publications/working_papers/GuyRobersWorkingPaper.pdf, 10.

against Estonia, Georgia, and Ukraine. Yet regardless of whether NATO chooses to construct a new center of excellence, it is imperative that it develop an organizational cyber offensive capability for defense, like its adversaries and key Allies (Germany, France, the UK, and the United States)[484] already have. NATO's current posture is all shield, with no sword in the cyber domain. This is not an astute or sustainable policy.

2. Cyber Cooperation

Information-sharing within the cybernetic domain remains critical to the Alliance's long-term defense, effectiveness, and preparedness for cyberwar. In this regard, the Alliance hosts countless multilateral exercises, workshops, and regional initiatives that encourage information-sharing and collaboration by private, public, and government stakeholders. NATO's cooperative security approach is also exemplified in the organization's commitment to improving its partnerships with the EU, the UN, and private actors. With its progressive and determined outlook on cyber, NATO is moving in a positive direction toward preparedness for cyberwar. Today, NATO's level of cyber cooperation makes it highly prepared to cybernetically address and counter major acts of cyber aggression against one or more of the Allies.

Yet, although the Alliance has expanded its cyber partnerships and enhanced cooperation in the field of science and technology, the Allies must invest more in their national critical infrastructure, IT management, and cybersecurity protocols in order to enhance their cyber defense and response capabilities. Additionally, NATO must continue to broaden its information-sharing so that it can more efficiently leverage and employ its diversity as a political means of potency. Expanding cyber cooperation with the EU, including the European Union Agency for Network and Information Security (ENISA), through mutual information exchanges, collaborative workshops, and exercises would enhance NATO's overall level of cyber preparedness. If the Allies worked more cohesively among themselves, with private industry, and with European national cyber authorities, they would not only cultivate higher cybernetic standards of readiness, but also further augment their existing capacity for deterrence and defense.

---

484 *National Security Strategy,* Her Majesty's Government, 24, 41.

3. Decision Making

NATO's decision-making procedures present unique challenges for a 28-member organization modelled on consensus. Although the precepts of Article 5 afford NATO with a myriad of collective defense options—to include cybernetic, economic, intelligence, diplomatic, and military measures—the rapid changing nature of hybrid warfare necessitates faster decision-making. For this reason, NATO's decision-making apparatus is moderately prepared to respond to major acts of cyberwar.

Currently, a decision to deploy a Rapid Reaction Team (RRT) to assist an Ally that has incurred a cyber intrusion must be reached by the North Atlantic Council (NAC), which could take days. NATO could reduce this decision-making time by mirroring the approach that the Supreme Headquarters Allied Powers Europe (SHAPE) employs to accelerate operational planning and approval. According to staff officers at SHAPE (from the author's conversations in Brussels, Belgium, September 16, 2015), the organization developed Graduated Response Plans (GRP) to enhance NATO's crisis response capability. NATO could adopt a similar system for its cyber divisions by developing pre-packaged cyber readiness plans, which would be pre-approved by the NAC; the plans would delegate RRT or Computer Emergency Response Team (CERT) deployment authority to the NATO Computer Incident Response Capability (NCIRC) Center or other cyber divisions in the case of an act of cyberwar against one or more of the Allies. Delegating a greater degree of responsibility to NATO's cyber institutions would accelerate the operational decisions that might be delayed at the strategic level of the NAC. Delegation would also streamline the Alliance's cyber response and execution capability to ensure that Allies that request support receive it before a cyber assault builds to the level of a major attack. This methodology would complement NATO's current defense adaptive approaches and make it more prepared to address significant attacks in cyberspace.

4. Political Will

Because domestic politics steer state behavior within international affairs, public sentiment often influences national policy and decision making at the strategic level.

Prior to voting on any political and military action, especially a use of force, the Allies will generally first consider the impact to their domestic climates. Declines in political will, as suggested by some public opinion surveys, have minimally prepared NATO to respond effectively to major acts of cyber aggression with military force. To ensure that an Ally that requires collective defense protection receives robust support from its fellow Allies, NATO must take the necessary steps to improve public understanding of its collective purposes within each member state.

NATO's Public Diplomacy Division, Public Affairs office, and Headquarters Consultation, Control and Communications Staff (HQC3) must work closely with the NATO Strategic Communications Center of Excellence in Riga, Latvia to improve messaging throughout and beyond the Alliance. Specifically, these agencies must focus on public opinion in the states that, according to some polls, had the least resolve to honor their responsibilities under Article 5 of the Washington Treaty. This thesis concurs with the original recommendations of NATO strategy expert Jamie Shea—that NATO must take definitive steps to educate Allied populaces on the defense necessities of the Alliance.[485] Domestic politics should not impede the Alliance from honoring its collective defense commitments. For now, NATO is not politically primed to respond effectively to major acts of cyberwar due to the inadequacy of its strategic messaging. Indeed, the Allies must first outmaneuver their adversaries within information campaigns if they are to defeat them in the cyberwarfare domain.

5. Crisis Management

Throughout each of NATO's four major combat operations to date, the missions, objectives, geopolitical contexts, and results were different. Operationally, NATO met its defined objectives during the Bosnia and Kosovo conflicts, but performed less optimally in fostering a sustainable environment of stability. NATO's coalition performances in the Bosnia and Kosovo conflicts against symmetric threats revealed proficiencies in short-term strategic planning, which allowed it to play to its strengths and employ its unmatched air striking power and strategic lift capability. In

[485] Shea, "NATO: The Challenges Ahead," 5.

contrast, NATO's operational performance deteriorated when it took action against irregular threats, like Taliban clansmen in Afghanistan and Gaddafi-regime loyalists in Libya, within regions that required a form of reconstruction that was outside NATO's core competencies and defense objectives. NATO is ill-equipped to operate in fragmented nations that do not have the political culture and institutional and civil infrastructure necessary to function as states. Both Libya and Afghanistan require a state-building capacity that only the European Union, the United Nations, non-governmental organizations, and national reconstruction agencies may have.

In the future, if cyber aggression leads NATO to consider military force, the Alliance would probably be more successful in conducting a campaign against a symmetric or semi-symmetric threat than an irregular one. If NATO's adversary is asymmetric or operating in an ethno-sectarian region that would require significant post-war state-building, the Alliance would be better off keeping the operation in the cybernetic domain. Aside from issues with political will, it would be acutely challenging for the Alliance to finance any large-scale crisis management interventions, given downward defense spending trends.[486] NATO's crisis management procedures and performance have minimally prepared the Alliance to effectively manage, sustain, and win in a cyberwar that evolves into a conventional war. In the event of a cyberwarfare campaign of aggression that rose to the level of Article 5, NATO might be more effective in managing the threat through cybernetic means than through kinetic military measures.

6. Defense Spending

NATO's leading member states—France, Germany, Italy, the UK, and the United States—are emerging from austerity measures and defense cuts at varying paces. While defense spending is gradually increasing, most of these nations are still operating against a backdrop of resource constraints. France, Germany, Italy, and the UK, which are also EU members, are in violation of the Maastricht Treaty's economic

[486] Shea, "Keeping NATO Relevant," 3.

guidelines, which restrict national debt to 60 percent of GDP.[487] France, Italy, the UK, and the United States all have debt levels that are at least 89 percent of their economic output levels.[488] Moreover, GDP growth for all five nations in 2015 averaged less than 1.7 percent, with the highest growth in Germany at 2.1 percent and the lowest in Italy at 1.0 percent.[489]

Nevertheless, despite high deficit levels and economic stagnation, the significant increase in cyber defense spending of France, the UK, and the United States shows that these Allies value cyber readiness as a categorical imperative. Moreover, if an act of cyber aggression led to an invocation of Article 5, the defense investments of France, the UK, and the United States would probably put these Allies in a stronger position to support a NATO-led intervention. Declines in defense spending juxtaposed with growing cyber defense budgets within prominent Allied states have moderately prepared NATO to effectively counter cyber aggression through cybernetic channels and military force. In the event of war initiated through cyberspace, NATO would likely be prepared to respond with armed force, but some Allies would be economically less prepared to sustain operations. The Alliance must firmly encourage its members to meet minimum defense spending guidelines, instead of only encouraging the Allies to "aim to move toward" the 2 percent of GDP standard.[490] Additionally, NATO must actively promote stronger national investments in cyber defense among the Allies. Expanding NATO's strategic messaging campaign within Allied member states would also assist in these endeavors, since defense spending is directly tied to political will.[491]

---

487 Kirk, "European Debt Crisis," 1.

488 Kirk, "European Debt Crisis," 1.

489 "Germany GDP Annual Growth Rate," Trading Economics, accessed March 21, 2016, http://www.tradingeconomics.com/germany/gdp-growth-annual, 1.

490 "Wales Summit Declaration," par. 14.

491 Shea, "NATO: The Challenges Ahead," 5.

7. Defense Policy Prioritization

France, Germany, Italy, the UK, and the United States have similar defense readiness goals and threat priorities but heterogeneous defense postures. France, the UK, and the United States have active defense postures that support their standing as national powers. Each of their defense policies underscores national ambitions and the need for strong, adaptable, innovative, and ready militaries that can project power, intervene internationally in support of Western values and interests, and cooperate with Allies and partners in coalition operations. Each of these three Allies has been consistent and vocal in demonstrating its commitment to NATO solidarity and collective defense. France, the UK, and the United States have demonstrated that, while expressions of support from international institutions and coalitions are valued aids to legitimacy, all three powers are prepared to act autonomously to support perceived national priorities. Germany and Italy, on the other hand, pursue defense policies that rely to a greater extent upon restraint and the critical backing and authorization of the United Nations Security Council (UNSC) and occasionally NATO (as with the Kosovo conflict of 1999).

As for cyber defense, the defense policies of France, the UK, and the United States focus strongly on cyber readiness and on how cyber incidents could spill over into the kinetic dimension. In the case of cyber aggression that escalated into conventional operations, France, the UK, and the United States would be the Allies most prepared to support a NATO intervention. If Germany and Italy supported a NATO-led operation, their contributions would most likely take the form of logistic or periphery support due to capability and fiscal constraints. In the event of war initiated through cyberspace, NATO would be prepared to respond with armed force, but economically less prepared to sustain operations in a protracted scenario. The defense policies of NATO's leading Allies have moderately prepared the Alliance to effectively address and counter cyberwar aggression through cybernetic means and military force.

B. SUMMARY

No one can predict exactly how NATO would respond to a major act of cyberwar against one or more of its members. The Allies have a menu of options available that they can employ to respond collectively in cyberspace or beyond. Although a NATO response to a major act of cyberwar would depend on the geopolitical considerations of each case, Article 5 invocation is most likely when the following four conditions are present: (1) the cyber aggression is performed in the integrity and/or availability domains, (2) the severity of the damage meets the threshold of an armed attack, (3) attribution can be confirmed without a compromise of cybernetic capability, and (4) the cyber act is either terrorist or state-sponsored.

The Alliance is more prepared cybernetically than it is politically, militarily, and economically to respond to a terrorist or state-sponsored cyber attack on one or more of the Allies. NATO is highly prepared to address, resolve, and counter major acts of cyberwar in the cybernetic dimension, but it is minimally prepared to respond to these threats with political and military measures. Although NATO might be able to promptly counter cybernetic aggression with force, it would be less fiscally able to sustain military operations effectively in the post-conflict phases. While patterns of defense policy prioritization and spending do not provide a comprehensive metric for measuring a state's defense readiness, they do offer an imperfect indicator of how prepared the Allies would be to support and contribute to a NATO-led intervention over an incident begun in cyberspace. The Alliance faces its most serious challenges with public support and crisis management that could make it less effective if it responded with force to cyberwar waged against its members. Nevertheless, if an Ally invoked Article 5 over a major act of cyberwar—political, economic, and defense constraints aside—the Allies would come to each other's collective aid.

The prospect of cyberwar presents a unique opportunity for NATO to strengthen its leadership role in the cybernetic domain, broaden its cyber cooperation with external stakeholders, enhance its decisional delegation practices, improve its strategic messaging, and increase defense spending. If the Alliance takes these critical steps, it will be better positioned and highly prepared to address the challenges resulting from

the evolving complexity and heterogeneity of incidents in cyberspace.[492] Until then, the Alliance remains moderately prepared for cyberwar, and this is not good enough for the most valuable collective defense organization in the world. As a leading security guarantor, NATO must continue to advance its cyber preparedness today if it is to remain relevant to Euro-Atlantic peace and security tomorrow.

[492] Buckland, Schreier, and Winkler, "Democratic Governance Challenges," 18–19.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albanese, Chiara, and John Follain. “A Prime Minister, a Referendum, and Italy’s Turn to Get Worried.” Bloomberg. July 4, 2016. http://www.bloomberg.com/news/articles/2016-07-04/a-prime-minister-a-referendum-and-italy-s-turn-to-get-worried.

Ambinder, Marc. “Cyber Attacks in Afghanistan. *The Week*, April 2, 2013. http://theweek.com/articles/466007/cyberattacks-afghanistan.

Archick, Kristin. *The European Union: Current Challenges and Future Prospects* (CRS Report No. R44249). Washington, DC: Congressional Research Service, 2016. https://www.fas.org/sgp/crs/row/R44249.pdf.

Armed Forces Communications and Electronics Association, The. *The Evolution of U.S. Cyber Power.* Accessed August 13, 2016. http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf.

Bajpai, Prableen. “The World’s Top Economies.” Investopedia. Last modified July 18, 2016. http://www.investopedia.com/articles/investing/022415/worlds-top-10-economies.asp.

Ball, Gregory. “Operation Allied Force.” Air Force Historical Support Division. August 23, 2012. http://www.afhso.af.mil/topics/factsheets/factsheet.asp?id=18652.

Barber, Tony. “Renzi is the Last Hope for the Italian Elite.” *Financial Times*, January 2, 2015. http://www.ft.com/intl/cms/s/0/21f3bf46-86cd-11e4-9c2d-00144feabdc0.html#axzz43Q9c9qW9.

Barfi, Barak. “What’s Really Holding Libya Back.” NATO Review, 2014. http://www.nato.int/docu/review/2014/Also-in-2014/Security-political-problems-Libya/EN/index.htm.

Bat Blue. *Terror Goes Cyber: The Cyber Strategies and Capabilities of Al Qaeda, ISIS, Al Shabaab, and Boko Haram.* April 2015. http://www.batblue.com/wp-content/uploads/2015/04/BatBlueReport_TerrorGoesCyber.pdf.

BBC. “Bosnia-Herzegovina Profile-Overview.” March 25, 2016. http://www.bbc.com/news/world-europe-17211937.

———. “Trump Presidency ‘Would Make World Less Safe’—Ex NATO Boss.” August 15, 2016. http://www.bbc.com/news/election-us-2016-37090988.

Begg, Iain, Fabian Mushovel, and Robin Niblett. “The Welfare State in Europe: Visions for Reform.” Chatham House. September 2015. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150917WelfareStateEuropeNiblettBeggMushovel.pdf.

Bendavid, Naftali. “Just Five of 28 NATO Members Meet Defense Spending Goal, Report Says.” *Wall Street Journal*, June 22, 2015. http://www.wsj.com/articles/nato-calls-for-rise-in-defence-spending-by-alliance-members-1434978193.

———. “Opinion in NATO Countries Varies Widely on Russia, Ukraine.” *Wall Street Journal*, June 10, 2015. http://www.wsj.com/articles/opinion-in-nato-countries-varies-widely-on-russia-ukraine-1433909106.

Bender, Jeremy. “France’s Military is All Over Africa.” *Business Insider*, January 22, 2015. http://www.businessinsider.com/frances-military-is-all-over-africa-2015-1.

Brooke-Holland, Louisa. “The 2015 SDSR: A Primer.” House of Commons. November 19, 2015. http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7235.

BSA. “Country: Germany.” Accessed March 19, 2016. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf.

Buckland, Benjamin S., Fred Schreier, and Theodor H. Winkler. “Democratic Governance Challenges of Cybersecurity.” DCAF Horizon 2015 Working Paper no. 1. http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security.

Bundeswehr. “Debate over German Defense Budget Surfaces.” May 21, 2016. http://www.dw.com/en/debate-over-german-defense-budget-surfaces/a-19275360.

Carayannis, Elias G., David F. J. Campbell, and Marios Panagiotis Efthymiopoulos, *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice*. New York: Springer, 2014.

Caton, Jeffrey L. *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications*. Carlisle Barracks, PA: United States Army War College Press, 2014.

CCDCOE. “Cyber Security Training Events.” Accessed August 27, 2015. https://ccdcoe.org/events.html.

CCDCOE. “NATO Summit Updates Cyber Defense Policy.” October 24, 2014. https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html#footnote3_buq6aol.

Chollet, Derek, Ben Fishman, and Alan J. Kuperman. “Who Lost Libya? Obama’s Intervention in Retrospect.” *Foreign Affairs*, May/June 2015. https://www.foreignaffairs.com/articles/libya/2015-04-20/who-lost-libya.

Clapper, James R. “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community.” Office of the Director of National Intelligence, 2013. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-090.pdf.

———. “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community.” Senate Armed Services Committee: Washington, D.C., 2016. https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

CNN. “2008 Georgia Russia Conflict Fast Facts.” March 21, 2016. http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/.

Cohen, Lenard. “Nationalism, the Kosovo Crisis, and Political Change in Serbia.” July 7, 2011. https://www.wilsoncenter.org/publication/164-nationalism-the-kosovo-crisis-and-political-change-serbia.

Cornell University Law School. “18 U.S. Code § 2331—Definitions.” Accessed August 1, 2016. https://www.law.cornell.edu/uscode/text/18/2331.

Cuddington, Danielle. “Support for NATO is Widespread among Member Nations.” Fact Tank. July 6, 2016. http://www.pewresearch.org/fact-tank/2016/07/06/support-for-nato-is-widespread-among-member-nations/.

Daalder, Ivo H. “Decision to Intervene: How the War in Bosnia Ended.” Brookings Institution. December 1, 1998. https://www.brookings.edu/articles/decision-to-intervene-how-the-war-in-bosnia-ended/.

Daly, John C. K. “Counterterrorism or Neocolonialism? The French Army in Africa.” *Terrorism Monitor,* 12, no. 5 (2014). http://www.jamestown.org/regions/africa/single/?tx_ttnews%5Btt_news%5D=42051&tx_ttnews%5BbackPid%5D=55&cHash=8e372fe5ecd8a63b4cfccecb1544d46e#.V7AtE5grK01.

Defense Ministry of the French Republic. *50 Years of Operations in Africa (1964-2014).* Cahier du RETEX—Research. April 2016. http://www.cdef.terre.defense.gouv.fr/content/download/5870/75552/file/20160606_50-ans-d-OPEX-Afrique_US.pdf.

Defense Ministry of the French Republic. *French National Digital Security Strategy.* October 19, 2015. http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

Department of Defense. “Kosovo/Operation Allied Force After Action Report.” Report to Congress. January 31, 2000.

De Selding, Peter B. “Paris Attacks Pressure French Defense Budget as New Space Programs Ramp Up. *Space News,* November 19, 2015. http://spacenews.com/paris-attacks-pressure-french-defense-budget-as-new-space-programs-ramp-up/.

Economist Intelligence Unit, The. “E-readiness Rankings 2008: Maintaining Momentum.” 2007. http://graphics.eiu.com/upload/ibm_ereadiness_2008.pdf.

———. “France’s Military Ties with Africa Strengthen.” May 21, 2014. http://country.eiu.com/article.aspx?articleid=1801832364&Country=Chad&topic=Politics.

Efthymiopoulos, Marios Panagiotis. “NATO’s Cyber-Defense: A Methodology for Smart Defense” in *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice*. Ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos. New York: Springer, 2014.

Federal Ministry of Defense. *White Paper 2006: On German Security Policy and the Future of the Bundeswehr.* 2006. http://responsibilitytoprotect.org/Germany_White_Paper_2006.pdf.

———. *White Paper 2016: On German Security Policy and the Future of the Bundeswehr.* 2016. https://cle.nps.edu/access/content/group/cebb1f88-2b49-4223-8047-b53ee880fc91/Germany-White-Paper-2016.pdf.

“France to Invest 1 Billion Euros to Update Cyber Defenses.” *Reuters*, February 7, 2014. http://www.reuters.com/article/france-cyberdefence-idUSL5N0LC21G20140207.

Freedberg, Sydney J., Jr. “NATO Hews to Strategic Ambiguity on Cyber Deterrence.” Breaking Defense. November 7, 2014. http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/.

Gallis, Paul. *NATO’s Decision-making Procedure* (CRS Report No. RS21510). Washington, DC: Congressional Research Service, 2003. fas.org/man/crs/RS21510.pdf.

Global Firepower. “Defense Budget by Country.” Accessed March 11, 2016. http://www.globalfirepower.com/defense-spending-budget.asp.

Goldberg, Jeffrey. “The Obama Doctrine.” *The Atlantic*, April 2016. http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/.

Greenberg, Jon. “Sanders Oversimplifies U.S. Share of NATO.” April 19, 2016. http://www.politifact.com/truth-o-meter/statements/2016/apr/19/bernie-s/sanders-oversimplifies-us-share-NATO/.

Hale, Henry. “Divided We Stand: Institutional Sources of Ethno-federal Survival and Collapse.” *World Politics* 56, no. 2 (January 2004).

Healey, Jason. “Cyber Attacks Against NATO, Then and Now.” *The Atlantic Council*, September 6, 2011. http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now.

Healey, Jason, and Klara Tothova Jordan. “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.” Atlantic Council. September 2014. http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf.

Healey, Jason, and Leendert van Bochoven. “Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO.” *Atlantic Council*, (2012). Washington, DC: The Atlantic Council of the United States. http://www.atlanticcouncil.org/images/files/publication_pdfs/403/NATO%20Cyber%20Warning%202012.pdf.

Hendrickson, Ryan C. “Crossing the Rubicon.” *NATO Review*, 2005. http://www.nato.int/docu/review/2005/issue3/english/history.html.

Her Majesty’s Government. *National Security Strategy and Strategic Defense Security Review: A Secure and Prosperous United Kingdom.* 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (2011): 49–60. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

Hichkad, Ravi R., and Christopher J. Bowie. “Secret Weapons & Cyberwar.” Armed Forces Journal, (2012). http://www.armedforcesjournal.com/secret-weapons-cyberwar-2/.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*, (2011). http://webcache.googleusercontent.com/search?q=cache:s3_Eq_P0o4AJ:smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf+&cd=1&hl=en&ct=clnk&gl=us.

Hughes, Rex. “NATO in Cyberspace: Digital Defenses.” World Today 65, no. 4 (April 2009).

iCasualties. “Operation Enduring Freedom.” Accessed March 25, 2016. http://icasualties.org/oef/.

Ira, Kumaran. “France Boosts Military Spending, Recruits More Youth into the Army.” May 23, 2015. https://www.wsws.org/en/articles/2015/05/23/fran-m23.html.

IT Pro. “Spending Review: Chancellor Confirms £1.9bn Cybersecurity Funding.” November 25, 2015. http://www.itpro.co.uk/security/25657/spending-review-chancellor-confirms-19bn-cybersecurity-funding.

Jennen, Birgit, and Rainer Buergin. “Merkel Seeks Security Spending Boost in Budget Driven by Crises.” Bloomberg. March 22, 2016. http://www.bloomberg.com/news/articles/2016-03-22/merkel-seeks-defense-boost-in-german-budget-driven-by-crises.

Jones, Ken M. “Cyberwar—The Next Frontier for NATO.” Master’s thesis, Naval Postgraduate School, 2015.

Jones, Sam. “NATO Top Brass Urges Political Leaders to be as Ready as Soldiers.” *Financial Times*, August 7, 2016. http://www.ft.com/cms/s/0/0455dcb2-55a7-11e6-9664-e0bdc13c3bef.html#axzz4HVXxHOKq.

Kirchgaessner, Stephanie. “Will Italy be Europe’s Next Casualty as Renzi Risks All on Referendum?” *The Guardian*, August 6, 2016. https://www.theguardian.com/world/2016/aug/06/matteo-renzi-italy-referendum-banks-brexit.

Kirk, Ashley. “European Debt Crisis: It’s Not Just Greece That’s Drowning in Debt.” *The Telegraph*, June 29, 2015. http://www.telegraph.co.uk/news/worldnews/europe/greece/11705720/European-debt-crisis-Its-not-just-Greece-thats-drowning-in-debt.html.

Klimburg, Alexander, ed. *National Cybersecurity Framework Manual*. Tallinn: NATO CCDCOE, 2012. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

Kofman, Michael and Matthew Rojansky. “A Closer Look at Russia’s ‘Hybrid War.’” *Kennan Cable*, no. 7 (2015): 1–8, https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

Kramer, Franklin D. “Achieving International Cyber Stability.” *Atlantic Council*, 2012. http://www.atlanticcouncil.org/images/files/publication_pdfs/403/kramer_cyber_final.pdf.

Krause, Hannes. “NATO on its Way Towards a Comfort Zone in Cyber Defense.” *The Tallinn Papers*, no. 3 (2014). https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_03.pdf.

Landay, Jonathan S. “20 Years after War Began, Bosnia Grows More Divided.” *McClatchy Newspapers*, April 25, 2012. http://www.mcclatchydc.com/news/nation-world/world/article24728359.html.

Libicki, Martin C. “Brandishing Cyber Capabilities.” RAND National Defense Research Institute (2013). http://www.rand.org/pubs/research_reports/RR175.html.

Limnell, Jarno. “Putin is Waging a Relentless Cyberwar Against Ukraine.” *Newsweek*, January 11, 2016. http://www.newsweek.com/putin-cyberwar-ukraine-russia-414040.

LookingGlass. “LookingGlass Cyber Threat Intelligence Group Links Russia to Cyber Espionage Campaign Targeting Ukrainian Government and Military Officials.” April 29, 2015. https://lgscout.com/press-release/lookingglass-cyber-threat-intelligence-group-links-russia-to-cyber-espionage-campaign-targeting-ukrainian-government-and-military-officials/.

Maass, Ryan. “France to Increase Defense Spending in 2016.” United Press International. October 2, 2015. http://www.upi.com/Business_News/Security-Industry/2015/10/02/France-to-increase-defense-spending-in-2016/4561443814370/.

MacAskill, Ewen. “International Force of 5,000 Prepares for Libya Deployment.” *The Guardian*, March 7, 2016. http://www.theguardian.com/world/2016/mar/07/international-force-ready-for-libya-deployment-as-terror-threat-fears-grow.

MacDonald, Neil, James Blitz, and Michael Steen. “Kosovo Ruling Seen as Boon to Separatists.” *Financial Times*, July 22, 2010. http://www.ft.com/cms/s/0/d4da3fa2-959d-11df-a2b0-00144feab49a.html#axzz4Jm990pTN.

Major, Claudia and Christian *Molling. German Defense Policy in 2014 and Beyond: Options for Change.* Notes du Cerfa, 113. Paris: Study Committee for Franco-German Relations. June 2014. https://www.ifri.org/sites/default/files/atoms/files/ifri_noteducerfa113majorandmollingeng.pdf.

Mashal, Mujib and Andrew E. Kramer. “Russia Pulls Back from Cooperating with U.S. on Afghanistan.” *New York Times*, February 20, 2016. http://www.nytimes.com/2016/02/21/world/asia/russia-pulls-back-from-cooperating-with-us-on-afghanistan.html?_r=0.

McMaken, Ryan. “Hey Big Spender: France’s Robust Military Spending.” Mises Wire. November 17, 2015. https://mises.org/blog/hey-big-spender-frances-robust-military-spending.

Michel, Leo. “NATO Decision Making: Au Revoir to the Consensus Rule?” *Strategic Forum*, no. 202 (2003). Institute for National Strategic Studies National Defense University. https://www.ciaonet.org/attachments/12787/uploads.

———. “Why Americans Should Worry about Marine Le Pen.” Atlantic Council, December 2015. http://www.atlanticcouncil.org/blogs/new-atlanticist/why-americans-should-worry-about-marine-le-pen.

Milne, Richard. “Trump’s Baltic Shift Sends Shivers through Region’s Capitals.” *Financial Times*, August 1, 2016.

Ministry of Defense of the Republic of Italy. *White Paper for International Security and Defense*. 2015. http://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf.

Minkoff, Yoel. “U.K. Inflation Gets Post-Brexit Boost.” Seeking Alpha. August 16, 2016. http://seekingalpha.com/news/3203602-u-k-inflation-gets-post-brexit-boost?ifp=0&source=email_wsb&utoken=3c2dc8ae2e2c23ed12620e168ca55b40.

Morbin, Tony. “NATO: Defending Against the Known Unknowns.” *SC Magazine UK*, 2015, http://www.scmagazineuk.com/nato-defending-agains-the-known-unknowns/article/400190/.

Mueller, Karl P., ed. “Precision and Purpose: Airpower in the Libyan Civil War.” 2015. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR676/RAND_RR676.pdf.

Nakashima, Ellen. “Chinese Government Has Arrested Hackers it says Breached OPM Database.” *Washington Post*, December 2, 2015. https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

NATO. “Afghan Managers Train in Cyber Defense.” May 21, 2012. http://www.nato.int/cps/en/natolive/news_86990.htm.

———. “Allied Command Operations (ACO).” Last modified November 11, 2014. http://www.nato.int/cps/en/natolive/topics_52091.htm.

———. “Collective Defense—Article 5.” March 22, 2016. http://www.nato.int/cps/en/natohq/topics_110496.htm.

———. “The Consultation Process and Article 4.” March 17, 2016. http://www.nato.int/cps/en/natohq/topics_49187.htm.

———. “Cyber Defense Pledge.” July 8, 2016. http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

———. “Cybersecurity.” Last modified July 9, 2015. http://www.nato.int/cps/en/natohq/topics_78170.htm.

———. “Defending the Networks: The NATO Policy on Cyber Defense.” 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

———. “Defense Expenditures of NATO Countries (2008-2015).” January 28, 2016. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160129_160128-pr-2016-11-eng.pdf#page=6.

———. “Enhanced Cyber Defense Cooperation in the South Caucasus and Black Sea Region.” July 29, 2015. http://www.nato.int/cps/en/natohq/news_121969.htm.

———. “Exercise Steadfast Cobalt Tests NATO’s Communications Systems.” June 4, 2015. http://www.aco.nato.int/exercise-steadfast-cobalt-tests-natos-communications-systems-2.aspx.

———. “Funding NATO.” June 3, 2015. http://www.nato.int/cps/en/natohq/topics_67655.htm.

———. “Improving NATO Capabilities.” February 16, 2015. http://www.nato.int/cps/en/natohq/topics_49137.htm.

———. “ISAF Mandate.” Last modified April 29, 2009. http://www.nato.int/isaf/topics/mandate/.

———. “ISAF’s Mission in Afghanistan (2001-2014) (Archived).” September 1, 2015. http://www.nato.int/cps/en/natohq/topics_69366.htm.

———. “The Kosovo Air Campaign (Archived): Operation Allied Force.” October 13, 2015. http://www.nato.int/cps/en/natohq/topics_49602.htm.

———. “Kosovo Force (KFOR) Key Facts and Figures.” May 2015. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_05/20150508_1505-kfor-placemat.pdf.

———. “Men in Black—NATO’s Cybermen.” April 24, 2015. http://www.nato.int/cps/en/natohq/news_118855.htm.

———. “NATO and Libya (Archived).” November 9, 2015. http://www.nato.int/cps/eu/natohq/topics_71652.htm.

———. “NATO CIS Group Adds New Unit in Croatia.” April 7, 2014. http://www.aco.nato.int/nato-cis-group-adds-new-unit-in-croatia.aspx.

———. “NATO Communications and Information Agency (NCI Agency).” April 7, 2016. http://www.nato.int/cps/en/natolive/topics_69332.htm.

_____. “NATO Communications and Information Systems School: About Us—Mission.” Accessed August 27, 2015. http://www.nciss.nato.int/mission.php.

———. “NATO Communications and Information Systems School: Courses—Course Descriptions.” Accessed August 27, 2015, http://www.nciss.nato.int/courses_description.php.

———. “NATO’s Practical Support to Ukraine.” December 2015. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf.

———. “NATO Stands Firm in Support for Ukraine.” May 13, 2015. http://www.nato.int/cps/en/natohq/news_119420.htm.

———. “The North Atlantic Treaty.” April 4, 1949. Washington, DC, http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

———. “Operations and Missions: Past and Present.” July 12, 2016. http://nato.int/cps/en/natohq/topics_52060.htm?selectedLocale=en.

———. “Peace Support Operations in Bosnia and Herzegovina.” September 7, 2015. http://nato.int/cps/en/natohq/topics_52122.htm?selectedLocale=en.

———. *Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization.* NATO Summit. Lisbon, 2010. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

———. “Wales Summit Declaration.” September 5, 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

———. “Wales Summit Declaration on Afghanistan issued by Heads of State and Government of Allies and their International Security Assistance Force (ISAF) Troop Contributing Partners.” September 4, 2014. http://www.nato.int/cps/en/natohq/news_112517.htm.

———. “Warsaw Summit Communiqué.” July 9, 2016. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO Cooperative Cyber Defense Center of Excellence. “NATO CCDCOE Command Brief.” Tallinn, Estonia, January 8, 2015.

NATO Internship Program. “NATO Communications and Information Organization (NCIO).” March 11, 2011. http://www.nato.int/cps/en/natolive/71161.htm.

Newell, James. “Italy’s Looming Referendum is Giving PM Matteo Renzi Sleepless Nights.” August 15, 2016. http://theconversation.com/italys-looming-referendum-is-giving-pm-matteo-renzi-sleepless-nights-63844.

Nikitakos, Nikitas, and Panos Mavropoulos. “Cyberspace as a State’s Element of Power” in *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice.* Ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos. New York: Springer, 2014.

“Norway Army Says Faced Cyber Attack after Libya Bombing.” *ABS/ CBN News*, May 19, 2011. http://news.abs-cbn.com/global-filipino/world/05/19/11/norway-army-says-faced-cyber-attack-after-libya-bombing.

Owen, Robert C., ed. Deliberate Force: A Case Study in Effective Air Campaigning. Alabama: Air University Press, 2000. http://www.au.af.mil/au/awc/awcgate/au/owen.pdf.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, ed. "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities." Washington, DC: National Academies Press, 2009.

Petratos, Pythagoras. "Cybersecurity in Europe: Cooperation and Investment" in Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities, and Implications for Theory, Policy, and Practice. Ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos. New York: Springer, 2014.

Pietras, Jennifer. "Austerity Measures in the EU—A Country by Country Table." European Affairs. Accessed August 3, 2016. http://www.europeaninstitute.org/index.php/112-european-affairs/special-g-20-issue-on-financial-reform/1180-austerity-measures-in-the-eu.

Polity. "NATO and Operation Allied Force." Accessed March 24, 2016, https://www.polity.co.uk/up2/casestudy/NATO_and_Operation_Allied_Force.pdf.

Presidency of the Council of Ministers. Italy's National Strategic Framework for Cyberspace Security. 2013. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf.

Presidency of the French Republic. French White Paper: Defense and National Security. 2013. http://www.rpfrance-otan.org/White-Paper-on-defence-and.

———. White Paper: Defense and National Security: 12 Key Points. 2013. http://www.rpfrance-otan.org/White-Paper-on-defence-and.

Puyveld, Damien Van. "Hybrid War—Does It Even Exist?" NATO Review. 2015. http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/.

"Renzi Should Make a Hard Push for Stimulus." Financial Times. August 14, 2016. http://www.ft.com/cms/s/0/bb4f7be8-607f-11e6-b38c-7b39cbb1138a.html#axzz4HNax3eK4.

Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." International Affairs Review. Accessed May 16, 2016. http://www.iar-gwu.org/node/65.

Roberts, Guy B. "NATO'S Centers of Excellence: A Key Enabler in Transforming NATO to Address 21st Century Security Challenges." Working Paper. October 8, 2014. http://www.stanleyfoundation.org/publications/working_papers/GuyRobersWorkingPaper.pdf.

Rühle, Michael. “Security Policy as Symbolism.” *Berlin Policy Journal*, February 2016. http://berlinpolicyjournal.com/security-policy-as-symbolism/.

Russell, Alison Lawlor. *Cyber Blockades.* Washington, DC: Georgetown University Press, 2014.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press, 2013.

Shahani, Aarti. “Report: To Aid Combat, Russia Wages Cyberwar against Ukraine.” April 28, 2015. http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.

Shea, Jamie. “Keeping NATO Relevant.” *Carnegie Endowment for International Peace*, (2012).

———. “NATO: The Challenges Ahead.” *Global Affairs* (2015). http://www.tandfonline.com/doi/full/10.1080/23340460.2015.979542.

“Significant Cyber Incidents since 2006.” Washington, DC: Center for Strategic and International Studies, 2016. https://www.csis.org/programs/strategic-technologies-program/cybersecurity/significant-cyber-incidents.

Sternstein, Aliya. “The Military’s Cybersecurity Budget in 4 Charts.” *Defense One.* March 16, 2015. http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/.

Stoltenberg, Jens. “NATO and Cyber Attacks: Time to Raise Our Game.” *The Parliament*, July 29, 2016. https://www.theparliamentmagazine.eu/blog/nato-and-cyber-attacks-time-raise-our-game.

———. *The Secretary General’s Annual Report 2015.* NATO. 2015. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160128_SG_AnnualReport_2015_en.pdf.

Suleyman, Anil. “NCIRC (NATO Computer Incident Response Capability).” 11 TF-CSIRT Meeting. Madrid, Spain. January 15, 2004. https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf.

Szabo, Stephen F. “Germany’s Commercial Realism and the Russia Problem.” *Survival: Global Politics and Strategy* 56:5 (2014): 117–128. doi: 10.1080/00396338.2014.962799.

Taylor, Adam. “That Time Ukraine Tried to Join NATO—and NATO Said No.” *Washington Post*. September 4, 2014. https://www.washingtonpost.com/news/worldviews/wp/2014/09/04/that-time-ukraine-tried-to-join-nato-and-nato-said-no/.

Thomas, Timothy L. “Al Qaeda and the Internet: The Danger of ‘Cyber-planning.’ *Parameters*, Spring 2003. http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf.

Tirpak, John A. ed. “Deliberate Force.” *Air Force Magazine*, October 1997. http://www.airforcemag.com/magazinearchive/documents/1997/october%201997/1097deliberate.pdf.

Trading Economics. “British Pound.” Accessed August 16, 2016. http://www.tradingeconomics.com/united-kingdom/currency.

———. “Germany GDP Annual Growth Rate.” Accessed March 21, 2016. http://www.tradingeconomics.com/germany/gdp-growth-annual.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia,” *The Guardian*, May 16, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

“Ukraine Crisis: Timeline of Major Events.” *The Telegraph*, March 5, 2015. http://www.telegraph.co.uk/news/worldnews/europe/ukraine/11449122/Ukraine-crisis-timeline-of-major-events.html.

U.S. Joint Chiefs of Staff. *The National Military Strategy of the United States of America*. Washington, DC, 2015. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

Verton, Dan. “Serbs Launch Cyber Attack on NATO.” FCW. April 4, 1999. https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx.

Walker, Andrew. “What’s the Problem with Italian Banks?” BBC. July 10, 2016. http://www.bbc.com/news/business-36708357.

Watson Institute for International and Public Affairs. “Costs of War.” Last modified March 2015. http://watson.brown.edu/costsofwar/costs/human/civilians/afghan.

White House, The. *Critical Infrastructure Security and Resilience*.” PPD-21. Washington, DC: Office of the Press Secretary, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

———. “Fact Sheet: European Reassurance Initiative and Other U.S. Efforts in Support of Allies and Partners.” June 3, 2014. https://www.whitehouse.gov/the-press-office/2014/06/03/fact-sheet-european-reassurance-initiative-and-other-us-efforts-support-.

“Who Recognized Kosovo as an Independent State?” Accessed March 25, 2016. http://www.kosovothanksyou.com/.

Williams, Thomas D. “Prime Minister Announces One Billion Euros for Security.” November 24, 2015. http://www.breitbart.com/national-security/2015/11/24/italian-prime-minister-announces-adding-1-billion-euros-for-security/.

Yost, David S. *NATO’s Balancing Act.* Washington, DC: United States Institute of Peace Press, 2014.

———. “The U.S. Debate on NATO Nuclear Deterrence.” *International Affairs* 87, no. 6 (2011).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California